8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción. Análisis de la actividad institucional del Área de Especialización**

El año 2015 ha venido a confirmar, como ya adelantábamos en anteriores memorias, la extraordinaria incidencia que los avances tecnológicos están teniendo en el ámbito de la delincuencia. El desarrollo de nuevas herramientas, su enorme capacidad y la utilización generalizada de las mismas por parte de todos los ciudadanos en cualquier lugar del mundo y al margen de cualesquiera circunstancias de carácter político, económico sociológico o cultural está determinando inimaginables oportunidades de prosperidad económica y social, de desarrollo científico y técnico, de expansión cultural y del conocimiento, de acercamiento entre los distintos pueblos y colectivos y, en definitiva, dando lugar a una imparable evolución en el planteamiento de las relaciones entre las personas, las instituciones e incluso los Estados. Sin perjuicio de ello, estos aspectos positivos tienen su contrapartida en los efectos perversos de un uso irregular de estas mismas herramientas aprovechando su enorme potencialidad para la planificación y ejecución de nuevas formas de acción criminal.

La plena conciencia de este fenómeno y de la repercusión que esa utilización irregular de estas nuevas herramientas puede tener –y en buena medida está teniendo– en el pleno ejercicio de los derechos y las libertades de las personas, está impulsando en los últimos años un claro empeño de muchos Estados y de diversas organizaciones internacionales en articular de forma coordinada soluciones legales que, plenamente respetuosas con los principios y valores que informan el Estado de Derecho, resulten adecuadas y eficaces en la acción policial y judicial frente a estas novedosas manifestaciones criminales. Esta acción coordinada es la única respuesta posible ante un fenómeno criminal que se desarrolla en el ciberespacio, más allá de límites territoriales y fronterizos y cuyos artífices se sirven de las diferencias en los ordenamientos jurídicos nacionales para dificultar su persecución y sanción y, en definitiva, procurar su impunidad.

De acuerdo con este planteamiento y en plena sintonía con los países del entorno más próximo, en nuestro país se publicó en el año 2013, la Estrategia Nacional de Ciberseguridad, en la que se fijaron las directrices para el uso seguro del ciberespacio *con una visión integradora a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas, contando además, con el sector privado y con los ciudadanos*. Uno de los objetivos de este documento, el ter-

cero de ellos, se refiere específicamente al tema que nos ocupa pues se concreta en *potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio*.

Para el desarrollo de estos objetivos a través de la elaboración de nueve planes derivados correspondientes a las distintas áreas de actuación se articularon diversos grupos de trabajo, en los que ha participado activamente la Unidad Central de este área de especialización, particularmente en los relativos a la definición del marco legal para la lucha contra la ciberdelincuencia y el ciberterrorismo y a la potenciación de la cooperación internacional. En dichos planes derivados que fueron aprobados el 14 de julio del pasado año 2015 por el Consejo Nacional de Ciberseguridad y posteriormente, el día 20 de julio por el Consejo de Seguridad Nacional (CSN) presidido por S. M. el Rey, se recogen –entre otras líneas de actuación– propuestas de reforma legislativa, algunas de las cuales ya han sido asumidas por el legislador español y publicadas en el último periodo anual, así como también iniciativas de acción formativa de operadores jurídicos e investigadores, parte de ellas dirigidas a los integrantes del Ministerio Fiscal.

Íntimamente vinculada a este planteamiento se encuentra la publicación en el año memorial de dos importantísimas reformas legislativas que afectan plenamente al ámbito de la ciberdelincuencia. Por una parte la del Código Penal llevada a efecto por las leyes orgánicas 1/2015 y 2/2015, ambas de 30 de marzo que, en lo que aquí interesa, incorporan tipos penales novedosos con los que se pretende hacer factible la persecución penal de determinadas manifestaciones criminales surgidas al socaire de la evolución tecnológica y también adaptan figuras delictivas tradicionales en el derecho patrio a las especialidades detectadas en las formas comisivas como consecuencia de la utilización de herramientas TIC en la planificación y ejecución criminal. En ambos casos, y en línea con lo anteriormente indicado, ha de reseñarse que muchas de estas modificaciones derivan de la implementación en el ordenamiento jurídico español de normas internacionales sobre la misma materia. Así ocurre con la Directiva 2013/40/UE de 12 de agosto sobre ataques a los sistemas de información, inspirada a su vez en la Convención de Budapest del Consejo de Europa, cuya incorporación al CP además de servir para la reorganización sistemática de los delitos de descubrimiento y revelación de secretos y daños informáticos, ha dado lugar a la tipificación de conductas como la interceptación ilegal de las transmisiones de datos entre sistemas (artículo 197.bis.2) y el abuso de dispositivos (artículo 197 ter y 264 ter) así como a la reelaboración de los subtipos

agravados y a la elevación de las sanciones respecto de los delitos de daños informáticos.

La adaptación de nuestra normativa interna se ha dejado notar igualmente en los delitos contra la libertad e indemnidad sexual de los menores, por influencia en este caso de la Directiva 2011/93/UE sobre abuso, explotación de los menores y pornografía infantil y de la Convención de Lanzarote del Consejo de Europa. La publicación de la LO 1/2015 ha implicado modificaciones en la figura del *child grooming* (artículo 183 ter), así como en los delitos de pornografía infantil (artículo 189), entre las que han de destacarse la tipificación del acceso *on-line* a material de esta naturaleza, la previsión específica en el código penal de la retirada de contenidos ilícitos, la interrupción de servicios o el bloqueo de unos y otros por resolución judicial, o la formulación de un concepto legal de pornografía infantil. A su vez, la LO 2/2015 ha supuesto novedades significativas en la tipificación y sanción de los delitos de terrorismo (artículo 573 y ss.) con el objetivo, alguna de ellas, de facilitar la actuación penal frente al uso de Internet con fines terroristas de acuerdo, también en este aspecto, con las pautas marcadas internacionalmente y, en particular, las fijadas por la Decisión Marco 2008/919/JAI y la Resolución n.º 2178 de NNUU de 24-IX-2014.

En otros casos las variaciones en los tipos penales han venido determinadas por la necesidad de ofrecer respuestas legales ante algunos comportamientos surgidos al hilo del uso de las TIC y que se han entendido merecedores de un reproche penal poco factible con la previa regulación legal. Buen ejemplo de ello, es la tipificación de la cesión inconsentida de imágenes de carácter íntimo (artículo 197.7) y del acoso permanente a través de medios de comunicación (artículo 172 ter) o la redefinición de los delitos contra los derechos de propiedad intelectual cometidos a través de los servicios de la sociedad de la información que acoge en nuestro ordenamiento penal la doctrina Svensson fijada por el Tribunal de Justicia de la Unión Europea (TJUE) en sentencia de fecha 13-II-2014.

Esta importante modificación legislativa se ha completado con la inaplazable reforma de la Ley de Enjuiciamiento Criminal, particularmente la llevada a efecto por LO 13/2015 de 5 de octubre que alcanza, entre otras materias, a la investigación tecnológica. Al margen de otras consideraciones sobre las novedades incorporadas en el proceso penal, algunas de las cuales analizaremos más adelante en lo que afecta a los procedimientos sobre cibercrimen, ha de reconocerse el acierto del legislador español al abordar de forma detallada y completa la utilización de las herramientas e instrumentos tecnológicos como medios de

investigación criminal, materia en la que la regulación existente hasta ahora era claramente insuficiente –especialmente si tenemos en cuenta los derechos y libertades que pueden verse afectados por dichas técnicas de investigación– como ya habían puesto reiteradamente de manifiesto nuestros Tribunales y el propio Tribunal Europeo de Derechos Humanos (TEDH). El legislador además de incorporar al texto legal la doctrina que al respecto han ido elaborando el Tribunal Supremo y el Tribunal Constitucional para cubrir –en la medida de lo posible– las carencias legales, ha aprovechado también para incorporar a nuestro ordenamiento algunos mecanismos de investigación recogidos en disposiciones internacionales como es el caso de la orden de preservación de datos (artículo 588 octies) derivada de los artículos 16 y ss. de la Convención de Budapest del Consejo de Europa y cuyo objeto es evitar la destrucción de evidencias electrónicas en tanto se obtiene autorización judicial para el acceso a las mismas.

Todo este desarrollo legislativo implica un compromiso importante para el Ministerio Fiscal que se concreta, en fase de elaboración de los textos legales, en trasladar oportunamente al legislador nuestros conocimientos, sugerencias y opiniones –resultado de la experiencia diaria en la aplicación de las normas– acerca de las necesidades detectadas y las soluciones legales que resulten factibles y posteriormente, tras la publicación de la norma, en la labor orientada a la unificación de criterios para la interpretación y aplicación de los nuevos preceptos, que la Institución lleva a efecto en virtud del principio de unidad de actuación que inspira su funcionamiento interno por disposición del artículo 124 CE.

Desde el área de especialización en Criminalidad Informática, y en lo que se refiere al año memorial, se ha dado cumplimiento a dicho compromiso. Así, trasladamos nuestras reflexiones y estudios tanto en lo que se refiere a la tipificación/modificación de algunas conductas delictivas –en la última fase de elaboración del Código Penal– como en lo relativo a determinadas herramientas de investigación, particularmente y con resultado positivo, en la previsión de la orden de preservación de datos (artículo 588 ter octies)–aprovechando a dicho fin los estudios realizados con ocasión de las reuniones de la Convención de Budapest del Consejo de Europa– y también en aspectos parciales de la regulación de la técnica del agente encubierto *on-line* (artículo 282 bis) o en la correspondiente a las condiciones de acceso al proceso de los datos electrónicos almacenados (artículo 588 ter j).

A su vez, publicadas las mencionadas disposiciones legislativas, los nuevos preceptos han sido objeto de examen y reflexión conjunta tanto con ocasión de las Jornadas de Especialistas celebradas en

mayo del año 2015, centradas en el estudio de las modificaciones operadas en los tipos penales, como en las de los días 10 y 11 de marzo del presente año 2016 orientadas, por su parte, a valorar el alcance de las medidas de investigación tecnológica que incorpora la reforma procesal. A partir de este trabajo en equipo, el área de especialización ha preparado en el año 2015 dos documentos cuyo objetivo es reforzar la unidad de criterio en la interpretación y aplicación de algunos de los tipos penales afectados por la LO 1/2015, concretamente la Circular 8/2015 *sobre los delitos contra la propiedad intelectual cometidos a través de los servicios de la sociedad de la información*, publicada en diciembre del año pasado y un borrador de Circular sobre las modificaciones operadas en los delitos de descubrimiento y revelación de secretos y daños informáticos, que se encuentra pendiente de estudio y valoración por los órganos centrales de la Fiscalía General del Estado.

El entendimiento por parte del Ministerio Fiscal de que la lucha contra este peligroso fenómeno criminal exige de la coordinación de esfuerzos con las Administraciones Públicas y, en general, con los organismos y entidades públicos y privados con responsabilidad en este ámbito, ha determinado que desde la Unidad Central del área de especialización se cuiden especialmente este tipo de relaciones. Así, junto a nuestra participación, en el año 2015, en las múltiples sesiones de trabajo celebradas con los diversos actores implicados en la elaboración de los planes de desarrollo de la Estrategia Nacional de Ciberseguridad, han de reseñarse también los contactos periódicos con diversas entidades y organismos institucionales como el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC); la Agencia Española de Protección de Datos; el Instituto Nacional de Ciberseguridad (INCIBE) y la Secretaría de Estado de Telecomunicaciones dependientes ambos del Ministerio de Energía, Industria y Turismo; el Embajador en Misión Especial para la Ciberseguridad del Ministerio de Asuntos Exteriores y Cooperación; la Dirección General de Política e Industrias Culturales y del Libro, del Ministerio de Educación, Cultura y Deporte y el Centro Criptológico Nacional (CCN-CERT) enmarcado en el Ministerio de Presidencia, además de la relación permanente y sostenida con los distintos Cuerpos Policiales nacionales y autonómicos –a las que nos referimos con mayor detalle en otro apartado de esta memoria– y con la Subdirección General de Tecnologías de la Información y las Comunicaciones del Ministerio del Interior e igualmente con los distintos departamentos relacionados con esta materia en el Ministerio de Justicia. Todo ello ha servido para facilitar el intercambio de información y de las expe-

riencias y conocimientos necesarios, tanto de carácter jurídico como estrictamente técnicos, para potenciar y reforzar nuestra actuación ante estas novedosas manifestaciones criminales.

Por su parte nuestro compromiso con los ciudadanos y la voluntad de facilitar la aproximación del Ministerio Fiscal a los problemas que está generando el uso irregular de las tecnologías en los diversos ámbitos de la sociedad, ha impulsado también una fluida relación con el Consejo General de la Abogacía y con muchos de los Colegios Territoriales de Abogados, labor esta última de las que se han ocupado preferentemente los Delegados provinciales, así como con determinados operadores de comunicaciones y/o proveedores de servicio de la sociedad de la información, como Telefónica o Google; con asociaciones u organismos de carácter privado tales como la Asociación Profesional Española de Privacidad o la Asociación Internacional para la Protección de la Propiedad Intelectual e Industrial (AIPPI) y también con colectivos u organismos directamente afectados o representantes de víctimas de hechos ilícitos de esta naturaleza, entre ellos, entidades bancarias, asociaciones y ONGs orientadas a la protección de menores, entidades de gestión de derechos de propiedad intelectual, empresas catalogadas como infraestructuras críticas, etc.

Igualmente y con la finalidad de dar a conocer la actividad que desarrolla el Ministerio Fiscal en esta materia y de compartir experiencias y conocimientos con otros actores de la Ciberseguridad, se ha potenciado la participación activa de los integrantes del área de especialización y en particular de quienes integran la Unidad Central en actividades formativas y foros de debate organizados en el año memorial por diversos organismos e instituciones públicos y privados, centros docentes, académicos, universitarios o de formación de cuerpos policiales, así como en encuentros dedicados específicamente a esta materia como el XI Congreso Nacional de la Abogacía Española, el II Congreso ENATIC de Abogacía Digital o la 9.ª edición del Encuentro Internacional de Seguridad de la Información ENISE y la Conferencia Meridian, organizados respectivamente por INCIBE y CNPIC y celebrados en forma consecutiva, ambos en la ciudad de León.

La creciente preocupación internacional por la incidencia cada vez mayor de la ciberdelincuencia ha determinado también que la séptima ronda de evaluaciones mutuas en el marco de la Unión Europea (GENVAL), estuviera dedicada en el año 2015 a reflexionar acerca de los mecanismos establecidos en cada Estado Miembro para hacer frente a este fenómeno criminal. A dicho fin distintos departamentos de la Administración y otros organismos públicos entre ellos el Ministerio Fiscal –representado a estos efectos por la Unidad Central de Crimi-

alidad Informática y la de Cooperación Internacional– intervinieron en la cumplimentación de un extenso cuestionario en el que se facilitó al equipo evaluador información, entre otros temas, sobre las últimas reformas legislativas, la organización policial, judicial y del Ministerio Fiscal para afrontar estas manifestaciones criminales así como aspectos operativos concretos en referencia a las actividades delictivas objeto de análisis: delitos de pornografía infantil, ataques a sistemas informáticos y defraudaciones a través de las TIC. Celebrada la reunión de evaluación en el mes de junio su resultado ha sido favorable destacándose, entre otros aspectos positivos, el valor de la Red de Especialistas en Criminalidad Informática del Ministerio Fiscal.

En el mismo plano transnacional y sin pretensión de exhaustividad se ha de mencionar igualmente, la participación de miembros de la Unidad Central en las dos reuniones del T-CY de la Convención de Budapest del Consejo de Europa celebradas respectivamente en los meses de junio y diciembre del pasado año 2015 en la sede del citado organismo. En la primera de ellas y en la subsiguiente conferencia *Octopus*, tuvimos ocasión de explicar las reformas procesales en curso –en aquel momento– en España y la adecuación de las mismas a las directrices de la citada Convención del Consejo de Europa. Por su parte la segunda de ellas sirvió para la puesta en marcha de una nueva fase de evaluación acerca de la tipificación en los ordenamientos jurídicos internos de los Estados Parte de las figuras delictivas que contempla dicho Instrumento internacional en sus artículos 2 a 10. En definitiva, la finalidad de estas reuniones es la de impulsar la armonización de las legislaciones nacionales, a partir de las necesidades prácticas constatadas en el curso de las investigaciones, para hacer posible una actuación más coordinada y eficaz ante las acciones ilícitas vinculadas al uso de las TIC. Es por ello que la participación en este foro de quienes integran la Unidad Central del área de Especialización se considera de gran interés en orden a trasladar nuestra propia experiencia y aprovechar la que, a su vez, están adquiriendo los operadores jurídicos/investigadores de países de nuestro entorno más próximo.

En este mismo marco, aunque centrado en la UE, ha de reseñarse igualmente nuestra implicación en la articulación de la red de Fiscales de Criminalidad Informática que se está poniendo en marcha desde Eurojust para facilitar la coordinación de esfuerzos en esta materia, así como en el Grupo de Trabajo creado a nivel europeo para reforzar la actuación ante los delitos contra la propiedad intelectual e industrial cometidos a través de estas tecnologías que se reúne periódicamente en la ciudad de Alicante, y de la que forman parte un miembro de la

Unidad Central y el Delegado Provincial de Cádiz. Igualmente no puede dejarse de mencionar la participación del Área de Especialización, en el año 2015 en diversas iniciativas europeas orientadas a mejorar la colaboración y el intercambio de experiencias entre autoridades judiciales, como el Proyecto ITOM sobre comercio ilegal en la red en el que estuvimos representados por el Fiscal Delegado de las Palmas de Gran Canaria, o el Proyecto Proteus sobre suplantación de identidad y protección de víctimas en internet, en el que ha participado activamente la Fiscal Delegada de Cáceres.

Finalmente y ya en relación con ámbitos geográficos más amplios pero también de enorme interés para nuestro país –por los vínculos culturales y lingüísticos existentes– merece una especial mención la actividad celebrada en el mes de Octubre en Santa Cruz de la Sierra (Bolivia) y coordinada desde esta Unidad Central en colaboración con la Fiscalía de Portugal en el marco de la Asociación Iberoamericana de Ministerios Públicos. Dicha actividad reunió, con el patrocinio de AECID y por espacio de cinco intensos días, a representantes de los Ministerios Públicos, especializados en la lucha frente a los cibercrimitos, procedentes de diversos países iberoamericanos, con el objetivo inmediato de compartir conocimientos y experiencias al respecto pero con una clara proyección de futuro al constituir el germen de una red de puntos de contacto en las Fiscalías Iberoamericanas que facilite y potencie una colaboración efectiva en investigaciones de interés común. Este último objetivo se ha visto reforzado con la decisión adoptada en la Asamblea Iberoamericana de Ministerios Públicos celebrada los días 28 y 29 de octubre del mismo año, que avalando ese mismo planteamiento, acordó impulsar la articulación y puesta en funcionamiento de una Red Iberoamericana de Fiscales Especializados en Cibercriminalidad.

8.2 Análisis de diligencias de investigación y procedimientos judiciales incoados y acusaciones del Ministerio Fiscal en el año 2015

La información recabada desde los órganos territoriales del Ministerio Fiscal en relación con la actividad de la propia Fiscalía y de los órganos judiciales durante el año 2015, permite constatar que en dicho periodo se incoaron en todo el territorio nacional un total de 22.575 procedimientos judiciales sobre hechos delictivos incluidos en el ámbito de aplicación de la Instrucción 2/2011 *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informá-*

tica de las Fiscalías. El obligado contraste de este dato con el obtenido por igual concepto en el año precedente da cuenta de un ligero incremento, cifrado en un 9,93 %, en referencia a los 20.534 procedimientos registrados en 2014. Esta aparente estabilización en el volumen de incoaciones, especialmente si comparamos este índice con los correspondientes al incremento interanual en los periodos precedentes –21,82 % entre el año 2011 y 2012; 50,68 % entre 2012 y 2013 y 71,21 % entre 2013 y 2014– debe matizarse en la medida en que la entrada en vigor de la reforma procesal operada por ley 41/2015 de 5 de octubre, ha determinado que en muchos de los territorios provinciales, los cuerpos policiales desde primeros de diciembre del pasado año, dejaron de remitir a los órganos judiciales, por disposición del nuevo artículo 284.2 LECrim, aquellos atestados en los que no constara autor conocido y no concurriera ninguna de las excepciones previstas en ese mismo artículo. Son diversas las Fiscalías que atribuyen a esta circunstancia el descenso, a partir del mes de diciembre, en el volumen de copias de atestados policiales recibidos y, en consecuencia de procedimientos judiciales incoados, lo que explicaría la «ralentización» en ese último periodo del ritmo anual de nuevas incoaciones.

Sin perjuicio de analizar más adelante las consecuencias de esta decisión legislativa, es preciso dejar constancia de que la valoración de la evolución de la criminalidad, que debe ser abordada en la Memoria anual por disposición del artículo 9 de nuestro Estatuto Orgánico, difícilmente puede llevarse a efecto, al menos en la materia que nos ocupa, teniendo en cuenta exclusivamente los datos correspondientes a los procedimientos de autor conocido. Al margen de la imprecisión de ese concepto en referencia a hechos delictivos en los que la determinación del responsable criminal solo será posible a partir del seguimiento y rastreo de las huellas electrónicas que necesariamente dejan estas acciones, las características del fenómeno criminal que nos ocupa –compleja ejecución técnica, facilidades para la «anonimización» de la comunicación y dispersión territorial de la actividad delictiva y sus efectos– determinan que el volumen de investigaciones en los que cabría considerar no preceptiva la remisión del atestado a los órganos judiciales y al Ministerio Fiscal pueda llegar a ser muy elevado. Obviamente la ausencia de información que ello supone, no solo puede limitar de forma importante nuestra valoración sobre la evolución del fenómeno sino también –y ello tiene mayor relevancia– la posibilidad de trasladar al Gobierno y también a los órganos legislativos, las reflexiones de la Institución acerca de *las reformas convenientes para una mayor eficacia de la Justicia* en este ámbito.

Ha de recordarse al respecto, que una buena parte de la actividad desarrollada desde la puesta en funcionamiento de este área de especialización, ha estado orientada precisamente a constatar la incidencia real de este tipo de manifestaciones criminales, a partir de los datos facilitados por los Delegados provinciales y obtenidos como consecuencia del seguimiento y control de los diversos procedimientos incoados en los respectivos territorios. Esta información se encontraba, antes de la constitución de la red, dispersa en estadísticas parciales de origen policial elaboradas con parámetros no siempre coincidentes, lo que se explica por el carácter transversal del fenómeno y la propia indefinición del concepto de ciberdelincuencia, como corresponde a una realidad cambiante que va variando al ritmo del desarrollo de las tecnologías. El resultado del trabajo realizado por la Fiscalía desde la constitución de la red está a la vista y se ha ido ofreciendo en las estadísticas anualmente publicadas, como se hace también en esta Memoria respecto a 2015.

Ciertamente los datos con los que contamos no reflejan la totalidad de los expedientes incoados por las mismas dificultades antes indicadas y por las derivadas de las carencias existentes en los sistemas de registro informático y mucho menos pueden considerarse indicativos de la real incidencia del fenómeno que nos ocupa dado que la cifra de criminalidad oculta en estas tipologías delictivas sigue siendo muy elevada, entre otras razones, porque muchas de las conductas delictivas no son denunciadas por motivos diversos y no llegan por tanto a conocimiento de los cuerpos policiales ni de los órganos judiciales o la Fiscalía. Sin perjuicio de ello, la información estadística recopilada a partir de datos reales y sistematizada, de acuerdo con criterios uniformes, por el Ministerio Fiscal ofrece año a año una mayor precisión, lo que permite constatar la consolidación de los resultados obtenidos en las distintas áreas y obtener algunas conclusiones sobre la incidencia del fenómeno en su conjunto y en sus distintas manifestaciones y sobre posibles tendencias de futuro, que pueden ser aprovechadas en la definición de políticas criminales y/o en el diseño de reformas legislativas en esta materia.

Es por ello que estimamos necesario dejar constancia de que la falta de conocimiento por parte de este área de especialización del Ministerio Fiscal de aquellas denuncias y/o investigaciones en las que no sea posible concretar el autor puede implicar la pérdida de una información imprescindible para el pleno desarrollo de la labor que hasta el momento veníamos desempeñando en el ejercicio de las funciones encomendadas.

8.2.1 PROCEDIMIENTOS INCOADOS

Centrándonos en la información correspondiente al año 2015, el análisis detallado de los procedimientos judiciales incoados por hechos ilícitos de esta naturaleza es el siguiente:

Delitos informáticos		Procedimientos judiciales	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.).	1.009	4,47
	Acoso a través de TICs (art. 172 ter).	96	0,43
Contra la integridad moral	Trato degradante a través de TICs (art. 173).	226	1,00
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189).	767	3,40
	Acoso menores a través de TICs (art. 183 ter).	98	0,43
	Otros delitos c/libertad sexual a través TIC.	77	0,34
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter).	220	0,97
	Descubrimiento/revelación secretos a través TIC (art. 197).	597	2,64
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215).	254	1,13
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (art. 248 y 249).	18.201	80,62
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.).	276	1,22
	Delitos c/ servicios de radiodifusión/interactivos (art. 286).	27	0,12
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	295	1,31
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss.).	70	0,31
De falsedad	Falsificación a través de la TICs.	193	0,85
Contra Constitución	Discriminatoria a través TIC (art. 510).	40	0,18
Otros.		129	0,57
Total		22.575	100,00

En primer término y a efectos de asegurar una correcta comparación de esta información con la correspondiente a anteriores periodos anuales ha de indicarse que la modificación del Código Penal por LO

1/2015 de 30 de marzo, ha determinado la necesidad de incorporar a la estadística anual algunas novedosas tipologías delictivas o de modificar la formulación de otras, lo que ha generado alteraciones en los distintos apartados del cuadro adjunto que determinan que el contraste con los resultados de años precedentes ofrezca algunas variantes que precisaremos al analizar cada una de ellas. A esos mismos efectos, es también conveniente aclarar que aun cuando la reforma del Código Penal no entro en vigor hasta el 1 de julio del pasado año, los datos correspondientes al primer semestre del año se incorporan a la estadística anual adaptándolos a los parámetros establecidos para recoger las variaciones introducidas tras la citada reforma.

Los datos estadísticos adjuntos acreditan, al igual que en años precedentes, que el volumen más elevado corresponde, sin duda alguna, a los expedientes incoados por hechos ilícitos encuadrables dentro del concepto genérico de estafa, un total de 18.201 que suponen un porcentaje del 80,62 % sobre el total de los registrados en el periodo anual de referencia. Se detecta no obstante un ligero descenso en el índice porcentual respecto al año 2014, en el que los procedimientos por estas tipologías delictivas superaron el 84 % de los incoados. Este elevado porcentaje en las incoaciones por estas conductas ilícitas que, pese a sus variaciones, se mantiene como una constante en todos los ejercicios –75 % en 2012; 80,59 % en 2013 y 84,39 % en el año 2014– permite afirmar que, al margen de la mayor o menor exactitud de los cifras concretas obtenidas en este apartado, las conductas defraudatorias con su derivado efecto perjudicial en el patrimonio de las víctimas son, con amplia diferencia, los comportamientos que con mayor frecuencia determinan la presentación de denuncias por los ciudadanos.

Sin perjuicio de ello, la valoración correcta de estos datos, requiere de dos precisiones que también apuntamos en otros ejercicios. En primer término es importante conocer que dentro de este apartado se incluyen, a efectos estadísticos, una pluralidad de comportamientos ilícitos encuadrables, todos ellos, en el artículo 248 del Código Penal. Se trata de acciones ilícitas de naturaleza muy diversa, cada una de las cuales presenta dinámicas delictivas específicas y también problemas diferentes en su investigación y en la determinación de sus autores y cuya distinción a efectos estadísticos no estamos por el momento en condiciones de llevar a efecto.

Entre ellas, el volumen más relevante lo integran las estafas informáticas, en sentido estricto, sancionadas en el apartado 2.º del citado artículo 248, en el que se encuadran tanto las transferencias inconsentidas de activos patrimoniales realizadas mediante manipulaciones informáticas o combinando las mismas con técnicas de ingeniería

social (phising, pharming etc.) como las defraudaciones llevadas a efecto mediante la utilización irregular de tarjetas de crédito, débito o cheques de viaje o de sus numeraciones, en perjuicio de sus legítimos titulares, acciones estas últimas, conocidas vulgarmente con el nombre de *carding*. En uno y otro caso, se trata de las defraudaciones que más dificultades presentan en su investigación y en las que se obtienen peores resultados por lo que muchos de estos procedimientos se ven abocados al archivo. Ello es debido, en el primer caso, a que muchas de estas actividades ilícitas se desarrollan por grupos organizados desde –o a través– de terceros países con los que los cauces de cooperación internacional no son especialmente fluidos. La actuación en España se limita, en múltiples ocasiones, a la investigación y enjuiciamiento de las personas que actúan como *mulas* y que son las encargadas de recepcionar las transferencias y remitirlas a los artífices y coordinadores de la actividad defraudatoria y respecto de las cuales, en no pocas ocasiones, se encuentran dificultades para acreditar su conocimiento o la intencionalidad dolosa o imprudente de la participación criminal. Cierto es que en el último periodo anual, el área de especialización se ha implicado, en estrecha colaboración con los cuerpos policiales y con apoyo de Eurojust, en algunas operaciones transnacionales que tienen por objeto actuar contra los responsables de estas organizaciones, encargados del diseño y control de la actividad criminal. Sin duda esta es la vía adecuada para hacer frente a estas manifestaciones criminales pero por el momento los avances son todavía de carácter puntual.

En cuanto al llamado *carding*, las dificultades de investigación derivan de que el uso irregular de las tarjetas o de sus datos se lleva a efecto *on line*, o incluso físicamente, en establecimientos comerciales fuera de nuestras fronteras y por cuantías mínimas –aunque en múltiples operaciones materializadas en diferentes lugares– de tal forma que resulta inoperante acudir a mecanismos de cooperación internacional que hagan factible el esclarecimiento de los hechos o la determinación de sus autores.

Con todo, las tipologías defraudatorias cuya investigación resulta más eficaz son aquellas que, planteadas como estafas tradicionales, su ejecución y particularmente el engaño a las víctimas se lleva a efecto a través de las TIC o más concretamente de internet. Es el caso de las ventas u ofertas fraudulentas de servicios que se planifican y difunden a través de la red en las que, en muchas ocasiones, tanto los autores del hecho como los perjudicados se encuentran en nuestro país. La peculiaridad de estos supuestos es que los diversos perjudicados suelen encontrarse diseminados por el territorio nacio-

nal y por tanto denuncian el hecho en diferentes sitios, dando lugar a la incoación de procedimientos independientes en una pluralidad de órganos judiciales pese a que el perjuicio sufrido por cada uno de los afectados procede de una misma actividad criminal. Es evidente que, en estas circunstancias, la pretensión de unificar todos esos procedimientos en uno solo deriva generalmente en el planteamiento de cuestiones de competencia y en consecuencia en retrasos significativos en la tramitación procesal. En orden a solventar estas dificultades se está empeñando desde el área de especialización un serio esfuerzo –que detallaremos en otro apartado de esta memoria– para identificar los diversos procedimientos judiciales, en esa forma vinculados, y hacer posible su acumulación en el órgano judicial que resulte competente para ello, de tal modo que la respuesta del Estado de Derecho resulte eficaz y adecuada a la gravedad del delito y al perjuicio general causado.

Pues bien precisamente esta es la segunda de las precisiones que anteriormente anunciábamos como necesarias para valorar adecuadamente el altísimo porcentaje de expedientes por estafa que año a año computamos en nuestros registros informáticos. Nótese que aun derivados de una misma acción criminal y por tanto susceptible de acumulación posterior, cada una de las denuncias que presentan, de forma individualizada, los múltiples perjudicados por este tipo de comportamientos darán lugar a una anotación informática independiente que engrosa el total de las cifras estadísticas por este concepto.

Los delitos de descubrimiento y revelación de secretos cometidos a través de las TIC se hacen acreedores en el año 2015, de un análisis más detallado pues, no en vano, son preceptos afectados significativamente por la reforma del Código penal como consecuencia de la implementación de la Directiva 2013/40/UE sobre ataques a los sistemas de información. En lo que se refiere al descubrimiento y revelación de información, en sentido estricto, se trata de conductas que aun ubicadas en dos apartados diferentes de la estadística, entre los delitos contra la intimidad –aquellos que afectan a este derecho fundamental– o en los delitos contra el patrimonio y el orden socioeconómico –cuando está afectado un secreto de empresa– es evidente que responden en ambos casos a una misma dinámica delictiva, el conocimiento/apoderamiento irregular mediante herramientas tecnológicas de información reservada alojada en dispositivos o sistemas informáticos ajenos. El número de procedimientos incoados por hechos de esta naturaleza asciende en 2015 a 873 de los que 597 son encuadrables en el ámbito de protección de la intimidad personal y los 276 restantes afectaron a secretos de empresa. Ello supone un porcentaje

del 3,36 % del total de expedientes registrados en el año y un incremento del más del 53 % en relación con la anterior anualidad en la que, conjuntamente por ambos conceptos, obtuvimos la cifra de 561 expedientes. El dato, a nuestro entender, adquiere una especial relevancia no porque sea reflejo de un crecimiento en la actividad delictiva en este ámbito sino porque revela una mayor tendencia de los ciudadanos a la denuncia de este tipo de acciones.

En este apartado se encuadran las conductas, cada vez más frecuentes, relacionadas con la sustracción de fotografías, videos o material de carácter personal obtenidas a partir de accesos irregulares a dispositivos electrónicos de cualquier tipo, entre ellos teléfonos móviles, acciones que, en ocasiones, aparecen vinculadas a conductas posteriores de extorsión o coacción, lo que hace que algunas de ellas encuentren su acomodo en otros apartados de esta misma estadística. También se incluyen aquí algunas de las denuncias por difusión inconsentida de imágenes o grabaciones de carácter íntimo, obtenidas inicialmente con la anuencia de la víctima, cuya reciente tipificación en el artículo 197.7 ubica en este apartado comportamientos que hasta ahora incluíamos, cuando las circunstancias así lo permitían, entre los delitos contra la integridad moral. El carácter novedoso de esta figura, vigente únicamente los seis últimos meses del año, ha hecho imposible concretar la cifra específica de expedientes a que la misma ha dado lugar.

Íntimamente vinculados con estos delitos no solo por encuadrarse en el mismo capítulo del Código Penal, sino también por su frecuente relación medial, son los comportamientos de acceso ilegal a sistemas, interceptación ilegal de transmisiones de datos y abuso de dispositivos (artículo 197 bis y ter), en los que el bien jurídico protegido más que el derecho a la intimidad personal es la propia seguridad de los sistemas. La reciente tipificación de varias de estas figuras y la reubicación sistemática del más clásico acceso ilegal a sistemas –hasta ahora incluido en el artículo 197.3– hacen que los datos obtenidos por este concepto deban valorarse con cautela.

En el apartado de los delitos relacionados con ataques informáticos han de reseñarse igualmente los procedimientos incoados por delitos de daños, figuras también profundamente afectadas por la incorporación de la Directiva antes mencionada. Según nuestros registros, el número de expedientes por estos tipos penales ascendió en el año 2015 a 295, lo que supone un 1,31 % del total de los incoados en el año por hechos ilícitos vinculados al uso de las TIC y un incremento del 106 % respecto de la cifra obtenida por el mismo concepto el pasado año y del 250 % respecto a los 84 procedimientos incoados

en 2013. Tampoco en este caso el repunte debe interpretarse como un incremento de las actividades delictivas de esta naturaleza, ya que es públicamente conocido, a través de informes oficiales e incluso por difusión de los medios de comunicación, el elevado volumen de ataques informáticos detectados año a año y sus graves consecuencias. El problema, como hemos indicado en anteriores memorias, radica en que estos hechos no suelen ser objeto de denuncia, por razones reputacionales o por falta de confianza en las posibilidades de actuación del sistema judicial. Por ello es positivo que poco a poco se vaya percibiendo una tendencia creciente a trasladar estos hechos a los órganos de la jurisdicción penal cuando se constaten indicios de actividad delictiva, pues ello resulta necesario para garantizar una respuesta adecuada a estas conductas desde el Estado de Derecho.

La conveniencia de tomar conocimiento de estos ataques no solo tiene interés a efectos de la persecución penal de sus autores sino también con finalidades de carácter preventivo. Al respecto ha de recordarse la apuesta que desde la UE se está haciendo, a través de la Directiva NIS, sobre seguridad de las redes y la información, documento en fase de elaboración con el que se pretende obligar a determinados sectores de la actividad económica y social, tanto pública como privada, a comunicar a los organismos competentes los incidentes de seguridad de carácter relevante con el objetivo de poder prevenir actuaciones de similar naturaleza contra entidades del propio Estado afectado o de los restantes miembros de la Unión.

La referencia a los delitos de pornografía infantil es siempre obligada en este estudio memorial. No es necesario recordar la gravedad de estos comportamientos ni tampoco la incidencia que en las conductas relacionadas con la libertad e indemnidad sexual de los menores está teniendo el desarrollo tecnológico y la generalización en el uso de estas herramientas por parte de todos los ciudadanos. La preocupación generada al respecto está dando lugar a continuas modificaciones legislativas con las que reforzar la actuación frente a estas manifestaciones criminales, de lo que son buen ejemplo las últimas novedades, antes referidas, en nuestro Código Penal. Los registros por delitos de pornografía infantil ascendieron el pasado año a 767, lo que supone un incremento de un 32 % respecto de los datos obtenidos por este concepto en el año 2014 y un 47 % más que en 2013. El dato también merece una valoración positiva pues es reflejo de una mayor eficacia en la actuación frente a este tipo de comportamientos. Tras unos años en los que se venía detectando un descenso en el número de incoaciones motivado, en buena medida, por las dificultades técnicas de la investigación como consecuencia de una mayor sofisticación en los medios o formas

empleados para la distribución y consumo de material pornográfico, el repunte da cuenta de una mejora en ese ámbito que seguramente se verá reforzada en el futuro por la tipificación de nuevas conductas o la articulación de herramientas de investigación adecuadas fruto, en ambos casos, de las recientes reformas legislativas.

También se detecta un considerable incremento en los delitos de acoso a menores de 16 años través de las TIC, que evolucionan desde las 60 incoaciones de 2014 a las 98 del año memorial, un 63 % de incremento que es prematuro valorar si obedece a la modificación operada en el tipo penal, uno de cuyos aspectos es la elevación de edad de las posibles víctimas ampliando el ámbito de aplicación del precepto, o a una mayor incidencia de este tipo de conductas.

Antes de concluir este apartado resulta de interés reseñar que en conjunto –y sin computar cuantos de los 77 registros por otros delitos de esta naturaleza recayeron sobre menores de edad– los expedientes incoados por ilícitos contra la libertad e indemnidad sexual de los menores cometidos a través de las TIC ascendieron a un total de 865 –casi un 4 % del total de los incoados en el año memorial– lo que refleja un incremento del 35 % respecto del mismo resultado obtenido en 2014.

Otro dato significativo en la información estadística que analizamos, es el correspondiente a las conductas que suponen un atentado contra la libertad de las personas, concretamente el correspondiente a expedientes incoados por comportamientos amenazantes o coactivos a través de las TIC. La cifra se eleva a 1009 registros que junto con las 96 incoaciones por el nuevo delito de acoso permanente a través de estas tecnologías, tipificado en el artículo 172 ter, vigente desde el pasado 1 de julio, hacen un total de 1.105 registros, un 4,90 % del volumen de incoaciones por delitos vinculados al uso de estas herramientas. La cifra es especialmente llamativa si la contrastamos con los 249 y 527 registros efectuados respectivamente por esta clase de conductas en los años 2013 y 2014 y da cuenta de una clara tendencia ascendente en este ámbito. Corrobora esta misma tendencia el incremento en los delitos contra la integridad moral que sumaron 226 anotaciones, cifra también muy superior a las 130 incoaciones reseñadas en 2014 o las 160 del año 2013.

Son muchos los Fiscales Delegados que llaman la atención sobre estos comportamientos y sobre la cada vez más frecuente utilización de estas herramientas y, en particular, los dispositivos móviles para hostigar, humillar, acosar y ofender a otras personas, vulnerando su libertad, dignidad e intimidad. Se trata de acciones dirigidas con frecuencia contra personas especialmente vulnerables, como los menores de edad

y las mujeres víctimas de violencia de género, y que pueden llegar a ocasionar muy graves consecuencias dada la potencialidad invasiva de estas tecnologías y la posibilidad que ofrecen de mantener la situación lesiva de forma permanente y prolongada en el tiempo.

En cuanto a los delitos contra la propiedad intelectual, el volumen de procedimientos también se está viendo incrementado en las últimas anualidades, detectándose una tendencia alcista como resultado de la evolución desde las 32 anotaciones del año 2013 o las 58 de 2014 a las 70 registradas en el año memorial. La razón hay que buscarla en las nuevas posibilidades de actuación frente a la vulneración de estos derechos a través de los servicios de la sociedad de la información, derivadas de la doctrina fijada por el TJUE acerca de la interpretación de la conducta típica *comunicar*, así como de la redefinición de los tipos penales llevada a efecto por la LO 1/2015 y vigente desde el 1 de julio del pasado año.

Finalmente mencionar los 40 registros por procedimientos relativos a la difusión del discurso del odio o a la incitación de actos de tal naturaleza cometidos a través de las TIC. También en este ámbito se percibe la imparable incidencia de la utilización generalizada de estas herramientas con objetivos discriminatorios y de humillación y hostigamiento frente a los que son diferentes, y la necesidad de combatir duramente estas conductas para evitar que las enormes posibilidades que ofrecen estas tecnologías sean utilizadas perversamente poniendo en riesgo valores esenciales de nuestro Estado de Derecho como el pleno respeto a la dignidad de las personas y la vigencia del principio de igualdad de todos los seres humanos.

8.2.2 ACUSACIONES DEL MINISTERIO FISCAL

El número de Escritos de Acusación formulados por el Ministerio Fiscal en el año 2015 en procedimientos por delitos de cualquier naturaleza vinculados al uso de las TIC asciende a un total de 1.242, cifra que refleja un leve descenso, en un 2,58 % en relación con las 1.275 acusaciones presentadas en el año 2014 y cuyo detalle en atención a las distintas tipologías delictivas queda reflejado en el siguiente cuadro:

Delitos informáticos		Calificaciones	%
Contra la libertad	Amenazas/coacciones a través de TICs (art. 169 y ss. y 172 y ss.).	133	10,71
	Acoso a través de TICs (art. 172 ter).	4	0,32

Delitos informáticos		Calificaciones	%
Contra la integridad moral	Trato degradante a través de TICs (art. 173).	26	2,09
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189).	251	20,21
	Acoso menores a través de TICs (art. 183 ter).	23	1,85
	Otros delitos c/libertad sexual a través TIC.	28	2,25
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter).	19	1,53
	Descubrimiento/revelación secretos a través TIC (art. 197).	72	5,80
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215).	18	1,45
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249).	508	40,90
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.).	12	0,97
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286).	17	1,37
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	17	1,37
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.).	34	2,74
De falsedad	Falsificación a través de la TICs.	35	2,82
Contra la Constitución	Discriminatoria a través TIC (art. 510).	6	0,48
Otros.		39	3,14
Total		1.242	100,00

Como fácilmente se constata, el volumen más elevado de acusaciones corresponde a los delitos de estafa, al igual que en los años 2012, 2013 y 2014, representando en esta ocasión un porcentaje del 40,9 % del total de las elaboradas en la anualidad examinada. No obstante, en el año memorial se observa un descenso, en cifras absolutas, en el volumen de escritos de esta naturaleza por delitos de estafa lo que da cuenta de una tendencia ya observada en periodos anuales precedentes pues la cifra de 618 acusaciones formuladas en el año 2013 se vio reducida a 577 en el año 2014 y a la de 508, en números absolutos, en el año 2015.

Igual tendencia descendente se aprecia en referencia a los delitos de pornografía infantil, en este caso, con un índice a la baja de casi el

12% que se concreta en una diferencia de 34 escritos respecto de los presentados en el año 2014. Puede resultar llamativo que el incremento antes comentado en el volumen de incoaciones por hechos delictivos de este tipo no tenga su reflejo en el trámite de conclusiones provisionales, pero ello se explica fácilmente por la circunstancia de que, salvo en supuestos excepcionales, la tramitación de las causas no se culmina en el mismo año, por lo que el aumento antes referido tendrá su reflejo en las acusaciones que se presenten en años sucesivos. Al respecto es de interés reseñar, haciéndonos eco de las quejas de muchos de los Fiscales Delegados, el importante retraso que ya desde hace años se está detectando en los informes periciales de informática forense, al parecer debido a la falta de medios personales y materiales en los gabinetes científicos de los cuerpos policiales, problema cuya gravedad se agudiza tras la reforma por ley 41/2015 del artículo 324 de la norma procesal, que fija plazos limitados para la tramitación de los procesos penales.

El porcentaje de procedimientos por delitos de esta naturaleza en los que se llega a formular acusación es significativamente alto en relación con los incoados anualmente –un 32% en referencia a la cifra de incoaciones en el año memorial o un 43% si lo comparamos con las incoaciones del año 2014–. Esta circunstancia se explica porque las investigaciones suelen tener por objeto actos de consumo o distribución de material pornográfico y ocasionalmente de producción, que se desarrollan en o desde nuestro país y que se inician a partir de la detección de direcciones IP comprometidas, localizadas por los propios cuerpos policiales en el curso de sus pesquisas o bien facilitadas por terceros o por informaciones obtenidas de otros países. En estas condiciones resulta factible la identificación de la persona responsable de la conducta ilícita y, en definitiva su acusación y posterior enjuiciamiento como autor del delito.

Con las salvedades indicadas, las acusaciones por otras tipologías delictivas ofrecen significativos incrementos respecto del año 2014. Tal es el caso de los delitos contra la integridad moral –52%– y de los de descubrimiento y revelación de secretos –10%–, daños informáticos –54%– delitos contra la propiedad intelectual –41%– delitos de odio y discriminación –50%– y delitos de amenazas y coacciones –47%– y especialmente, los delitos de *child grooming* en relación con los cuales se observa un elevadísimo aumento del 130% respecto de los escritos de acusación a los que dieron lugar estas conductas en el año 2014.

Finalmente y para completar la información relativa a este apartado, hemos de precisar que las 39 acusaciones incluidas en el epí-

grafe *otros* engloban conclusiones provisionales sobre hechos ilícitos que, aun vinculados al uso de las TIC, no encuentran acomodo en otros apartados de la estadística anual, tales como las calificaciones formuladas por delitos de blanqueo de capitales –relativamente frecuentes en los supuestos de *phising*–, conductas de maltrato habitual en el marco de la violencia de género en los que el uso de las TIC ha sido determinante en el desarrollo de la acción criminal, delitos contra la propiedad industrial, etc.

8.2.3 DILIGENCIAS DE INVESTIGACIÓN

Terminamos este estudio de la actividad realizada por el Ministerio Fiscal en referencia a investigaciones criminales concretas con el análisis de los datos relacionados con las Diligencias de investigación que el Ministerio Fiscal incoa y tramita directamente al amparo de lo establecido en el artículo 5 de nuestro Estatuto Orgánico y del artículo 773-2.º de la LECrim. Es una vía de la que dispone la Institución para hacer efectiva una mayor implicación en las investigaciones criminales y canalizar las denuncias que cada vez con mayor frecuencia recibe la Fiscalía directamente de los ciudadanos o de otros organismos e instituciones de carácter público o privado.

Sin embargo, en el área de actuación que nos ocupa, el recurso a este clase de expedientes de carácter pre-procesal, se encuentra muy limitado, como ya hemos mencionado en anteriores memorias, por la circunstancia de que la identificación y posterior seguimiento de muchas de las *huellas* que dejan estas actividades delictivas, por incidir en derechos fundamentales de las personas, exigen de autorización judicial y en consecuencia de la remisión de nuestra investigación al órgano judicial competente en estricta aplicación de lo establecido en el artículo 773-2.º LECrim. Por ello, en muchas ocasiones, nos vemos abocados en trasladar la denuncia inmediatamente al Juzgado de Instrucción para poder iniciar la investigación o a judicializar nuestras actuaciones muy tempranamente, al ser imprescindible acceder a información cuya obtención exige dicho aval judicial.

Pese a este inconveniente, el número total de diligencias de investigación iniciadas en el año 2015, en todo el territorio nacional por hechos enmarcables en el ámbito de la ciberdelincuencia asciende a 95, con un incremento de casi el 46 % en referencia al año 2014. Este aumento en el volumen de incoaciones ha de valorarse muy positivamente en la medida en que, con las salvedades antes indicadas, da cuenta de que nuestro esfuerzo por aproximarnos a los ciudadanos y

en particular a las víctimas de estos comportamientos está ofreciendo resultados positivos dado que, con frecuencia cada vez mayor, los afectados por estos comportamientos se dirigen directamente a la Institución.

Delitos informáticos		Dil. investig.	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss.).	2	2,11
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189).	4	4,21
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter).	1	1,05
	Descubrimiento/revelación secretos a través TIC (art. 197).	10	10,53
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215).	10	10,53
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249).	11	11,58
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	4	4,21
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.).	3	3,16
Contra la Constitución	Discriminatoria a través TIC (art. 510).	50	52,63
Total		95	100,00

El volumen más elevado corresponde, sin duda, a las diligencias incoadas por delitos relacionados con los crímenes de odio que constituyen más de un 52,63 % de las registradas en el periodo anual objeto de esta Memoria. Este dato es reflejo de la importancia creciente que está teniendo internet y, en general las tecnologías de la información y la comunicación en la difusión del discurso del odio o en la incitación, facilitación o ejecución de acciones concretas motivadas por discriminación u odio hacia quienes pertenecen a determinados colectivos. Con mucha menor relevancia son también reseñables las 11 diligencias que tuvieron su origen en delitos de estafa y, en cifra similar, las incoadas por supuestas calumnias o injurias a autoridad o funcionario público en el ejercicio de sus funciones, así como las 10 correspondientes a delitos de descubrimiento y revelación de secretos, que suponen un 11,5 % en los dos primeros casos y el 10,5 % en el último, del total registrado en 2015.

Del conjunto de estas nuevas diligencias, un 54,7 % resultaron finalmente archivadas, en tanto que un 25,2 % dieron lugar, tras la

investigación del Fiscal, a la presentación de querrela o denuncia ante el órgano judicial competente. Las restantes, un 20 %, estaban en tramitación al finalizar el año memorial.

8.3 Relación con los Cuerpos y Fuerzas de Seguridad. Información sobre investigaciones criminales

Un año más ha de destacarse la extraordinaria y fructífera relación que la Unidad Central de este área de especialización mantiene con las Fuerzas y Cuerpos de Seguridad del Estado, que se manifiesta tanto en la colaboración en una diversidad de investigaciones concretas con proyección, en muchos casos, en todo el territorio del Estado, como también en las continuas reuniones de trabajo mantenidas con las Unidades especializadas de Policía Nacional y de Guardia Civil.

Esta colaboración se hace cada vez más necesaria para la adecuada orientación e impulso de las investigaciones en curso –dada la sofisticación de los medios comisivos que exigen del mutuo intercambio de conocimientos técnicos y jurídicos– especialmente tras la entrada en vigor de las modificaciones operadas durante el año memorial en el Código Penal y en la Ley de Enjuiciamiento Criminal y también para reflexionar conjuntamente, aprovechando la experiencia de unos y otros, acerca de alcance de tales novedades, fundamentalmente en relación con el elenco de medidas de investigación tecnológica que incorpora la reforma procesal; Así, en nuestras reuniones de trabajo con los expertos policiales estamos intercambiando conocimientos e información que hagan posible una adecuada interpretación de aspectos tales como lo que ha de entenderse por *proceso comunicativo*, a efectos de la habilitación necesaria para acceder a los datos conservados o cuál debe ser el contenido y alcance de las facultades reconocidas, al respecto, al Ministerio Fiscal y a la Policía Judicial y también sobre otros extremos de especial interés como la utilización de la técnica del registro remoto de sistemas informáticos, o de las facultades que otorga el artículo 282 bis LECrim al agente encubierto *on-line*. Nuestra pretensión es facilitar, de esta forma, la fijación de pautas uniformes en la aplicación de los nuevos preceptos, que contribuyan a hacer efectivo el principio de unidad de actuación recogido en el artículo 124 CE.

Las relaciones de los Delegados provinciales con los cuerpos policiales, nacionales y autonómicos, son igualmente positivas y fructíferas, siendo práctica habitual las reuniones conjuntas, para tratar de cuestiones técnicas así como para el seguimiento e impulso

de actuaciones concretas, con el fin de lograr el mayor éxito en la persecución de este tipo de delitos. Uno de los ejes esenciales sobre el que se ha articulado nuestra relación con las unidades policiales ha sido, precisamente, la transmisión de información sobre investigaciones en curso.

Hasta la reforma de la Ley de enjuiciamiento criminal por Ley 41/2015, de 5 de octubre, los Delegados han venido recibiendo copia de todos atestados referentes a esta materia. Como se hizo constar en memorias anteriores, uno de los principales objetivos del área de especialización ha sido, desde un principio, la identificación, para su posterior seguimiento y control, de los procedimientos incoados por hechos ilícitos vinculados al uso de estas tecnologías. Con ello se ha conseguido disponer de información cierta y debidamente contrastada acerca de la evolución de este fenómeno criminal en su conjunto y en sus distintas manifestaciones, así como de los datos necesarios para llevar a cabo la labor de coordinación de investigaciones que, relacionadas con una misma actividad criminal, producen sus efectos en distintos puntos del territorio nacional o incluso más allá de nuestras fronteras. No se trata solo, en consecuencia, de un control estadístico de la materia, sino que se pretende conocer la incidencia real de esta forma de delincuencia y hacer posible una investigación más eficaz de esos comportamientos, que, de no ser conocidos en su completa dimensión, en muchos casos podrían verse avocados al archivo.

Buena muestra de ello y de la utilidad de esta información es la incoación en la Unidad Central de un total de 26 Expedientes de Coordinación en el año 2015 a través de los cuales ha sido posible el conocimiento en su conjunto de hechos delictivos que afectan a diversas provincias y a una pluralidad de personas –superando una visión aislada y parcial de los efectos de una misma actividad ilícita– lo que está haciendo de estos expedientes el único mecanismo para hacer factible una respuesta jurídica adecuada ante esta clase de conductas. En estos casos ha sido precisamente la recepción de los atestados policiales por los Delegados provinciales lo que ha permitido detectar la existencia de hechos delictivos –especialmente ilícitos contra el patrimonio– que habían producido sus efectos en diversas provincias y que, por su escasa importancia individualmente considerada, podrían resultar intrascendentes a efectos penales. El análisis conjunto de los mismos ha hecho posible la visión completa del hecho criminal, el impulso y/o reapertura de los procedimientos y su acumulación en el órgano judicial competente. Es de interés indicar que el número de expedientes de esta clase, en abril de 2016, asciende a 17 lo que da

cuenta del incremento de la actividad de coordinación por parte de la Fiscalía y de su eficacia en la persecución penal de estas conductas.

Pues bien, esta importante labor puede verse significativamente afectada por la nueva regulación contenida en el artículo 284 LECrim, pues, como ya se ha avanzado, podría limitar la visión de conjunto que hasta ahora tenía esta área de especialización sobre el fenómeno que nos ocupa. El citado artículo recoge en su apartado primero la obligación de la Policía Judicial de *participar* inmediatamente a las autoridades judiciales y al Ministerio Fiscal cualquier hecho que revista caracteres de delito, pero indica en su apartado segundo que, como criterio general, no procederá la remisión del atestado –si bien se conservará a disposición de dichas autoridades– en los casos en que no conste autor conocido, sin perjuicio de las excepciones que se recogen en el mismo precepto. Entre tales excepciones se encuentra la de que el Ministerio Fiscal o la autoridad judicial soliciten la remisión del atestado.

La interpretación de este precepto merece una seria reflexión. En primer término ha de indicarse que esta nueva redacción del artículo 284 suscitadificultades interpretativas acerca de lo que ha de entenderse por *autor no conocido*, ya que cuando se trata de delitos cometidos a través de las TIC, la determinación de la identidad del responsable siempre es –al menos en hipótesis– si no plenamente conocida, *cognoscible* con el solo hecho de realizar el rastreo de las huellas electrónicas que necesariamente dejan estas acciones. Bastaría seguir esas huellas del delito para identificar al autor, seguimiento que en la mayor parte de los supuestos requerirá de autorización judicial con el fin de acceder, como primera medida, a los datos de tráfico asociados al proceso comunicativo, ex artículo 588 ter j LECrim. Pero además como el propio Informe del Consejo Fiscal al Anteproyecto de modificación de la norma procesal tuvo ocasión de señalar *la exclusión de la obligación de remisión por la Policía al Juzgado de Instrucción de la totalidad de los atestados sin autor conocido puede afectar al control jurisdiccional de la actividad de la Policía Judicial, que constituye una exigencia elemental del principio democrático de separación de poderes*. En consecuencia y, siendo el ciberdelincuente generalmente susceptible de identificación mediante la solicitud de un mandamiento judicial que haga posible el seguimiento de su rastro electrónico, no sería ilógico concluir que en los casos de delitos cometidos a través de las TIC, el atestado debiera siempre ser remitido al órgano judicial.

En todo caso, la reforma del precepto obliga necesariamente al área de especialización a redefinir las directrices marcadas a los res-

ponsables policiales sobre la remisión de atestados al Ministerio Fiscal, con la finalidad de que puedan seguir cumpliéndose los objetivos arriba indicados. A estos efectos, se considera imprescindible que se traslade al Ministerio Fiscal copia de todos los atestados que se remitan a los órganos judiciales por hechos ilícitos encuadrables en el marco de la ciberdelincuencia y en los que exista autor conocido, así como de las diligencias posteriores ampliatorias de los mismos. Igualmente debieran ser objeto de remisión los relativos a materias especialmente sensibles a los que se refiere expresamente el artículo 284.2 LECrim como de envío obligatorio aun cuando no exista autor conocido, entre ellos, los atestados sobre hechos que afecten a la libertad e indemnidad sexual de los menores, en los que se engloban los lamentablemente frecuentes delitos de pornografía infantil, *child grooming* o *sexting*.

Pero existen también algunas otras manifestaciones criminales de este fenómeno con incidencia en bienes jurídicos especialmente sensibles que también requerirían de un seguimiento específico y que, aplicando rígidamente el precepto que nos ocupa, pudieran quedar al margen del conocimiento por parte de la autoridad judicial o del Ministerio Fiscal. Entre ellos, y a modo de ejemplo, los derivados de ataques informáticos que, como se ha indicado, están experimentando un notable ascenso o los relativos a crímenes de odio o discriminación cometidos a través de internet, cuyo efecto lesivo en los derechos fundamentales de las personas es incuestionable. En uno y otro caso, por las circunstancias concurrentes y porque su comisión se lleva a efecto generalmente desde otros países o a través de prestadores de servicio radicados fuera de nuestras fronteras, se trata de actuaciones ilícitas en las que difícilmente podrá llegar a determinarse el autor, pero que desde el Ministerio Fiscal se estima irrenunciable conocer si queremos hacer efectiva la función de valoración y análisis que tiene encomendada la Institución por expresa disposición del artículo 9 del Estatuto Orgánico, en orden a informar a los poderes del Estado competentes sobre las medidas que se estiman más adecuadas u oportunas para la definición de las políticas criminales frente a estos graves y peligrosos comportamientos.

Es por ello que al menos debiera ser exigible que la Policía Judicial, dando cumplimiento a la obligación establecida en el artículo 284.1 LECrim de *participar* al Ministerio Fiscal la existencia de otros atestados en los que no exista, en principio, autor conocido ni vías que hagan factible su determinación posterior, efectuara una comunicación por escrito, de periodicidad al menos quincenal, en la que se relacionen, con el detalle necesario, la totalidad de actuaciones iniciadas,

la naturaleza del delito denunciado en cada supuesto y las circunstancias relativas a la imposibilidad de la determinación de la autoría del mismo. Ello permitiría al Delegado provincial solicitar, cuando fuere preciso a la vista de la relación recibida, la remisión de los atestados, que, a su juicio, fueren merecedores de una atención especial y de la incoación, si así se estima oportuno, de Diligencias de Investigación en la Fiscalía, para el esclarecimiento de los hechos y de las personas responsables de los mismos.

8.4 Estructura y funcionamiento de la Red de especialistas en Criminalidad Informática

La publicación de la Instrucción 1/2015 *sobre algunas cuestiones en relación con las funciones de los Fiscales de Sala Coordinadores y los Fiscales de Sala Delegados* ha dado carta de naturaleza a la actividad de los Fiscales que, destinados en Fiscalías de Área, colaboraban desde hace años con el Delegado Provincial de la especialidad, lo que venía sucediendo en distintos lugares del territorio nacional y particularmente en las provincias con mayor índice de población. La obligación derivada de dicha Instrucción de llevar a efecto el nombramiento de un Fiscal de enlace en todas las Fiscalías de Área supone un gran impulso para hacer posible el objetivo del control completo y pormenorizado de todas las causas por hechos ilícitos vinculados al uso de las TIC y, por ende, de la función de supervisión asignada al Delegado provincial con el objetivo de lograr la necesaria unidad de criterio del Ministerio Fiscal.

Esta circunstancia ha contribuido también a que la red de especialistas haya experimentado en el año 2015 un significativo crecimiento, no solo por el nombramiento de enlaces en todas las Fiscalías de Área sino también porque, aun no siendo obligatoria la designación de puntos de contacto en las Secciones Territoriales, no son pocos los Fiscales Jefes Provinciales que, a la vista del incremento de este fenómeno delictivo han optado, en algún caso desde hace años, por asignar a personas concretas responsabilidades en esta materia en las secciones territoriales e incluso en otros servicios especializados y porque también en muchas Fiscalías provinciales se ha incrementado el número de Fiscales que, aun sin dedicación exclusiva, se dedican a esta especialidad bajo la coordinación del Delegado provincial. Así, son actualmente casi 130 los Fiscales que trabajan, con o sin dedicación exclusiva, en este ámbito de actuación, lo que supone un incremento aproximado del 150% desde la puesta en marcha de la red.

Este aumento de Fiscales especializados ha supuesto también una mejora en la coordinación con otros servicios de la respectiva Fiscalía, especialmente con las secciones de menores y de violencia de género, áreas en las que se produce una masiva utilización de las TIC para la comisión de hechos delictivos. También se ha reforzado la relación con las secciones de cooperación internacional, pues el carácter transnacional de los ciberdelitos demanda de una estrecha colaboración entre autoridades judiciales y policiales para lograr una acción eficaz contra estas conductas. Esta visión omnicompreensiva de la materia permite la creación de sinergias entre los distintos servicios de la Fiscalía, compartiendo y aprovechando los conocimientos técnicos adquiridos en relación con ello.

La mencionada Instrucción ha supuesto también la atribución a quienes coordinan las áreas de especialización y, en particular la que nos ocupa de determinadas competencias que contribuyen al reforzamiento de la unidad de actuación del Ministerio Fiscal y a garantizar la máxima calidad técnico-jurídica en nuestra actuación. Así ocurre con el reconocimiento de la competencia de la Unidad para la labor de supervisión de los escritos de acusación que, si bien ya había sido acordada en las Jornadas de especialistas de los años 2012 y 2013, se ve ahora refrendada por la citada Instrucción, dando lugar en los escasos meses transcurridos desde su publicación a un considerable aumento de la actividad de la Unidad en este concreto aspecto. Igual efecto se pretende a través de la propuesta de elaboración de dictámenes para la resolución de consultas, cauce que puede resultar extraordinariamente útil y, así está siendo utilizado para facilitar la fijación de criterios en la interpretación de las novedades legislativas en esta materia.