8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción**

El uso de las tecnologías de la información y la comunicación (en adelante TIC) con fines delictivos es un fenómeno en constante evolución que enfrenta al legislador y también a los operadores jurídicos ante el desafío de ofrecer soluciones que resulten eficaces frente los nuevos comportamientos criminales o las nuevas manifestaciones o formas de comisión de conductas tradicionales vinculadas al desarrollo tecnológico, pero sin olvidar que dichas soluciones no deben limitar o restringir, en modo alguno, los derechos y las libertades fundamentales de los ciudadanos y los principios y valores inherentes al Estado de Derecho.

Respondiendo precisamente a ese desafío, el legislador español abordó en el segundo semestre del año 2015 importantes reformas legislativas, como las operadas en el Código Penal por las leyes orgánicas 1/2015 y 2/2015 ambas de 30 de marzo y la que se llevó a efecto en la Ley de Enjuiciamiento Criminal por la Ley Orgánica 13/2015, de 5 de octubre. Las primeras de ellas tuvieron por objeto, entre otras finalidades, tipificar nuevas conductas delictivas y/o adaptar las ya existentes a las formas de ejecución criminal surgidas al hilo de la evolución tecnológica. En cuanto a la ley orgánica 13/2015 su aportación más importante fue, sin duda, acomodar nuestra añeja norma procesal a las necesidades que plantea la investigación tecnológica. También alguna de las modificaciones en la Ley de Enjuiciamiento Criminal derivadas de la publicación de la Ley 41/2015 de 5 de octubre para la agilización de la justicia penal y el fortalecimiento de las garantías procesales ha incidido específicamente en el ámbito de actuación de esta especialidad como tendremos ocasión de detallar en esta misma Memoria.

La entrada en vigor de tan importantes y transcendentes reformas legislativas ha determinado que el año 2016 haya sido para el área de especialización en criminalidad informática del Ministerio Fiscal español un periodo marcado por la reflexión, el estudio y el debate interno acerca de la interpretación y aplicación de las figuras delictivas recientemente tipificadas o de las modificaciones incorporadas en los tipos penales ya existentes y también sobre las posibilidades que ofrece la utilización (plenamente ajustada a la legalidad) de las modernas técnicas de investigación reguladas en la norma procesal para el esclarecimiento de las múltiples manifestaciones de la ciberdelincuencia y la determinación de sus autores.

Fruto de este esfuerzo de análisis y reflexión conjunta, sobre la base de la experiencia adquirida con ocasión de la actividad diaria, por quienes integran la red de fiscales especialistas en criminalidad informática, fue la publicación, a finales del año 2015 de la Circular *sobre los delitos contra la propiedad intelectual cometidos a través de los servicios de la sociedad de la información*, que analiza las modificaciones producidas en dichas figuras delictivas tras la citada reforma penal. También responde a ese mismo esfuerzo la preparación, en el año memorial, del borrador de Circular sobre las modificaciones operadas en el indicado texto legal respecto a los tipos penales correspondientes a los delitos de descubrimiento y revelación de secretos y a los daños informáticos, que se encuentra pendiente de estudio y aprobación, en su caso, por la Junta de Fiscales de Sala. A su vez, en mayo de 2016 vio la luz el dictamen sobre *la valoración de las evidencias físicas o digitales aportadas al proceso penal como medios de prueba de comunicaciones electrónicas,* documento en el que, a partir de esa misma experiencia, se fijan criterios para la adecuada utilización en el proceso penal de las evidencias obtenidas de los dispositivos tecnológicos y de los medios de comunicación o transmisión digitales, telemáticos y/o electrónicos. Igualmente en el mismo periodo anual hemos elaborado otro dictamen (pendiente de publicación en el momento de elaborar este informe) relacionado, precisamente con alguna de las novedades incorporadas en la Ley de Enjuiciamiento Criminal por la ley orgánica antes mencionada. Se trata del dictamen sobre *el alcance de la reclamación de datos de identificación de titulares de terminales y/o dispositivos de conectividad prevista en el nuevo artículo 588 ter m) LECrim,* cuyo objeto es establecer criterios uniformes en la interpretación del citado precepto procesal.

Con todo, la imparable evolución tecnológica en la que nos encontramos inmersos determina que el proceso de adaptación de las normas legales a la realidad social no pueda darse por finalizado, ni siquiera momentáneamente. Buen ejemplo de ello es la publicación en el mes de mayo del pasado año del Reglamento europeo 2016/679 de 27 de abril *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos,* con el que se pretende ofrecer soluciones a los retos que plantea el desarrollo tecnológico y la globalización para el pleno ejercicio del derecho a la protección de los datos de carácter personal y cuya consecuencia más inmediata, a efectos internos, va a ser la modificación de nuestra Ley Orgánica 15/1999 de 15 de diciembre sobre esa misma materia, proyecto en el que ya se está trabajando desde la Agencia Española de Protección de Datos. Pues bien, íntimamente

vinculada a dicho Reglamento, ha de mencionarse la Directiva (UE) 2016/680 del Parlamento y del Consejo, también de 27 de abril, cuyo objetivo es cohonestar la adecuada protección de los datos de carácter personal con las necesidades de tratamiento y circulación de los mismos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones de dicha naturaleza. La incidencia de esta Directiva en las investigaciones y procedimientos penales de carácter transnacional es evidente, como la tendrá, también en esta materia, la Directiva 2014/41/CE del Parlamento y del Consejo *relativa a la Orden Europea de Investigación Penal,* de 3 de abril, también en periodo de implementación en nuestra normativa interna.

De otro lado ha de hacerse mención a la reciente publicación de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, 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 Directiva NIS. Si bien esta disposición normativa se centra especialmente en aspectos relacionados con la detección y prevención de ataques informáticos, su incorporación al ordenamiento jurídico español, que habrá de llevarse a efecto antes de mediados de mayo de 2018, va a tener también repercusión en la actividad del Ministerio Fiscal y particularmente en las responsabilidades de éste área de especialización. Ello es así porque en la citada directiva se establecen deberes específicos para una pluralidad de entidades, empresas u organismos (públicos o privados) que desarrollan su actividad en múltiples sectores de actividad económica y social (energía, banca, transportes y sanidad, entre otros) que se concretan no solo en la adopción de determinadas medidas de seguridad, sino también en la obligación de notificar a las autoridades competentes cualquier incidente de seguridad informática de efectos significativos que detecten con ocasión de sus respectivas actividades. Es evidente que buena parte de dichos incidentes pudieran presentar caracteres delictivos, si por sus circunstancias y características resultan incardinables en los artículos 197, 197 bis, 197 ter, 264, 264 bis o 264 ter CP, lo que daría lugar, en su caso, a la incoación de los correspondientes procedimientos penales.

No podemos dar por finalizada esta brevísima referencia a la evolución legislativa nacional y trasnacional relacionada con esta materia, sin referirnos expresamente a la reciente Sentencia de 21 de diciembre de 2016 dictada por el Tribunal de Justicia de la Unión Europea (Gran Sala) en los asuntos acumulados C-203/15 y C-698/15 en los que se resolvieron sendas cuestiones prejudiciales planteadas por el Tribunal

de Apelación de lo Contencioso-Administrativo de Estocolmo (Suecia) y el Tribunal de Apelación de Inglaterra y País de Gales. En dicha sentencia el TJUE se pronuncia acerca de la incidencia que puede tener en los derechos reconocidos en los artículos 7,8 y 11 de la Carta de Derechos Fundamentales de la Unión Europea (relativos respectivamente al derecho a la vida privada y familiar, protección de datos de carácter personal y libertad de expresión e información) la obligación de conservar de forma generalizada datos de tráfico de las comunicaciones y la posibilidad de acceder a los mismos en el curso de las investigaciones criminales, medidas ambas contempladas actualmente en la legislación interna de muchos de los países de la Unión. En particular y, en lo que se refiere a nuestro país, aun cuando todavía están por determinarse las consecuencias concretas que la doctrina fijada en dicha sentencia va a tener en la vigente Ley 25/2007 de 18 de octubre *sobre conservación de datos de las comunicaciones electrónicas y redes públicas de comunicación,* resulta incuestionable, a tenor de lo dispuesto en el art. 10.2 CE, su incidencia como criterio hermenéutico en la interpretación del sentido y alcance que ha de darse a dichos derechos y libertades reconocidos en nuestra Norma Fundamental.

8.2 Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en el año 2016

Los datos estadísticos que recogemos en este apartado ha sido obtenidos a partir de la información trasladada a la Unidad Central de Criminalidad Informática desde las Fiscalías Provinciales en referencia a los hechos ilícitos competencia de la especialidad, tal y como vienen delimitados en la Instrucción 2/2011 de la Fiscalía General del Estado *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías*. A partir de esa información se ha podido constatar que, en el año 2016 llegaron a conocimiento del Ministerio Fiscal, en el conjunto del territorio nacional, un total de 8.035 procedimientos de esta naturaleza. Dicho dato es reflejo de un descenso extraordinariamente llamativo (concretado en un 64,40 %) respecto de la cifra obtenida por este mismo concepto en el año 2015, en el que el número de procedimientos por hechos ilícitos competencia de la especialidad ascendieron a 22.575.

Es obvio que este resultado hace necesaria una explicación. Ha de recordarse, y así se ha puesto de manifiesto en anteriores memorias de esta área de especialización, que una de las mayores dificultades para

el análisis de este fenómeno criminal viene siendo la detección e identificación de los procedimientos judiciales/diligencias de investigación penal que tienen por objeto hechos ilícitos vinculados al uso de las TIC. Ello es debido a la transversalidad de este fenómeno criminal que puede manifestarse en comportamientos ilícitos de diversa naturaleza y encuadrables en una pluralidad de figuras delictivas, lo que determina que su reflejo estadístico quede, en ocasiones, oculto en los datos globales correspondientes al registro genérico de las diversas tipologías penales, salvo que se deje constancia específica del carácter informático de la infracción.

Precisamente por ello y para resolver este problema se ha venido empeñando, en los últimos años, un esfuerzo muy especial desde este área de especialización en el entendimiento de que la adecuada identificación y el control estadístico de estos procedimientos es de un incuestionable valor para el conocimiento de la incidencia y evolución en nuestro país de estas actividades criminales y para hacer factible una intervención *especializada* del Ministerio Fiscal en dichos procedimientos o, al menos, en aquellos que presenten una mayor transcendencia y complejidad.

En anteriores memorias hemos tenido la ocasión de explicar el sistema de trabajo establecido, en coordinación con las Fuerzas y Cuerpos de Seguridad, para adquirir ese conocimiento *temprano* de todas estas investigaciones y para hacer posible su anotación registral y el control y seguimiento de las mismas, a partir de la remisión a los servicios de criminalidad informática territoriales de las copias de todos los atestados incoados por hechos típicos de esta naturaleza. Ello nos ha permitido, entre los años 2011 a 2015, ir ampliando nuestro conocimiento –y también nuestra intervención– respecto a los procedimientos por delitos vinculados al uso de las TIC y como consecuencia de ello estar en condiciones de ofrecer algunas reflexiones acerca de la evolución de dicho fenómeno criminal, que aun siendo matizables a causa de nuestras propias limitaciones en la percepción de esa realidad, sirvieran para facilitar una información útil en orden a articular soluciones legales y operativas frente dichas conductas delictivas, tal y como nos encomienda el artículo 9 de nuestro Estatuto Orgánico.

Así en la memoria correspondiente al año 2011 pudimos ofrecer información acerca de un total de 6.532 procedimientos judiciales incoados durante ese periodo por hechos de esta naturaleza, cifra que se incrementó en un 21,82 % en el 2012; en un 50,64 % en el 2013 y en un 71,21 % en el 2014, anualidad en la que se alcanzó la cifra de 20.534 procedimientos registrados por este tipo de delitos. Esta incuestionable tendencia alcista se vio ralentizada de forma evidente

en el año 2015, en el que el incremento porcentual de estos expedientes fue solo del 9,93 %, cambiando drásticamente de signo en el año 2016 en el que hemos constatado la reducción en un 60,40 % en el número de incoaciones, que anteriormente hemos comentado.

Estos sorprendentes resultados en ningún caso han de interpretarse como un cambio de tendencia en el fenómeno criminal que nos ocupa. Contrariamente, la información, que aún de forma asistemática y parcial seguimos recibiendo de los ciudadanos, de las empresas y colectivos afectados y de las propias Fuerzas y Cuerpos de Seguridad y que bien puede ser utilizada como complemento de los datos que ofrecen nuestros registros estadísticos, da cuenta de un crecimiento progresivo de las acciones ilícitas vinculadas a las TIC, como consecuencia perversa de la creciente penetración de estas tecnologías en la actividad política, económica, cultural y social y en las relaciones entre los ciudadanos. Sin embargo, el reflejo de estas conductas en la actividad de los Tribunales y del Ministerio Fiscal se ha visto afectado, de forma determinante, por la reforma la Ley de Enjuiciamiento Criminal y, más concretamente, por la nueva redacción dada por Ley 41/2015, de 5 de octubre al artículo 284 del citado texto legal, en vigor desde el día 6 de diciembre del mismo año, a cuyo tenor los atestados incoados por los cuerpos policiales, en los que no conste autor conocido, no han de ser trasladados a la autoridad judicial ni al Ministerio Fiscal, salvo que concurran cualquiera de las excepciones previstas en los tres apartados contemplados en el número segundo del citado precepto procesal.

La aplicación de este precepto ha dado lugar a una reducción drástica en el volumen de diligencias policiales que llegan a conocimiento de los juzgados de instrucción y de las fiscalías por hechos ilícitos relacionados con el uso de las TIC cuyo alcance resume claramente ese índice descendente de casi un 65 % anteriormente comentado. Dicha circunstancia, a nuestro entender, puede generar unos efectos perversos no solo en las posibilidades de acción penal frente a este tipo de actividades delictivas, sino también en la correcta valoración del fenómeno criminal y en la adopción de las medidas legislativas o de orden práctico necesarias para responder adecuadamente ante el mismo.

Varias son las cuestiones sobre las que entendemos ha de reflexionarse. Así, en primer término, hemos de recordar que generalmente en estas actividades ilícitas aun cuando, en inicio, no se encuentre identificado el responsable de una concreta conducta, es posible su determinación posterior a partir del seguimiento y rastreo de las huellas que necesariamente dejan todas las comunicaciones electrónicas. Ciertamente habrá supuestos en los que el aprovechamiento en la dinámica

criminal de determinadas técnicas (uso de anonimizadores o de redes wifi ajenas o públicas, entre otras posibilidades) o la concurrencia de determinadas circunstancias fácticas o jurídicas (tales como la irrelevancia del perjuicio causado, la utilización de servidores extranjeros o la exigencia de requisitos de procedibilidad específicos) determinarán finalmente la imposibilidad y/o improcedencia de llevar a efecto esas labores de rastreo o seguimiento pero, aun en esos supuestos, dicha decisión implica una valoración que exige de ciertos conocimientos de carácter técnico o jurídico y, en consecuencia de una preparación adecuada para ello o al menos del establecimiento de unos criterios perfectamente definidos al respecto.

A esta imprecisión acerca de lo que ha de entenderse por autor desconocido en referencia a estos ilícitos, se une la circunstancia de que muchos de ellos y, en particular, los cometidos a través de la red pueden ejecutarse en sus diversas fases o producir sus efectos simultánea o sucesivamente en distintos lugares, por lo que no es infrecuente que aspectos parciales de una misma acción criminal se denuncien en lugares diversos dando lugar a una pluralidad de atestados que, analizados aisladamente, pudieran generar la falsa percepción de que no es posible la identificación de su autor o de que resultan injustificadas o improcedentes, por la escasa relevancia del resultado, la práctica de las actuaciones necesarias para ello.

Al riesgo efectivo de que, por la conjunción de circunstancias antedichas, dejen de ser investigados, y en consecuencia enjuiciados, hechos ilícitos susceptibles de serlo se une otro efecto, a nuestro entender negativo, de una inadecuada aplicación del art. 284 LECrim que es la pérdida de una información debidamente contrastada y unificada sobre la incidencia que está teniendo el uso de las herramientas tecnológicas en la actividad delictiva en nuestro país y, en definitiva, sobre la evolución del fenómeno criminal que nos ocupa. Dicha información entendemos puede tener un valor esencial en la definición de políticas de actuación o en la adopción de medidas legislativas u operativas para afrontar de forma más precisa y efectiva el riesgo que entrañan estas acciones criminales.

Como ya indicamos en memorias anteriores, uno de los objetivos que pretendía el Ministerio Fiscal con el control y seguimiento de los atestados/ diligencias/ procedimientos judiciales por acciones criminales de esta naturaleza era el de ofrecer una visión global acerca de dichos extremos, dado que los datos sobre denuncias o acciones ilícitas de esta naturaleza se encontraban, antes de la constitución de la red de especialistas en criminalidad informática, dispersos en estadísticas

parciales, normalmente de origen policial, estructuradas de acuerdo con parámetros no siempre coincidentes. Con esa finalidad hemos venido trabajando a los largo de los cinco últimos años con los resultados antes indicados y que se detallan en los informes correspondientes a los diferentes periodos anuales. El nuevo régimen de traslado de atestados, tal y como se viene aplicando desde finales del año 2015, reduce extraordinariamente la información que llega a conocimiento del Ministerio Fiscal y nuestras posibilidades de actuación en el sentido antes indicado.

Todas estas circunstancias han determinado que en éste área de especialización del Ministerio Fiscal se estén barajando diversas soluciones para solventar los problemas antes mencionados.

En primer término, parece imprescindible el establecimiento de pautas generales, comunes a los distintos cuerpos policiales, acerca de las circunstancias en las que ha de entenderse que no existe autor conocido en referencia aquellos hechos ilícitos que por haberse cometido a través de estas tecnologías suelen dejar un rastro susceptible de seguimiento. Al respecto hemos observado, a partir de la información ofrecida por las fiscalías territoriales, que la ausencia de esas pautas comunes está determinando valoraciones diferentes en los distintos cuerpos policiales o incluso, aun tratándose de una misma institución, en los diversos lugares del territorio nacional. Tal vez la intervención en esa primera fase de unidades policiales con un cierto nivel de especialización técnica pudiera contribuir a solventar buena parte de las disfunciones detectadas.

Por otro lado consideramos de interés se haga efectiva la obligación de «participar» al Ministerio Fiscal y a los órganos judiciales la incoación de todos los atestados relativos a este tipo de delitos, tal y como preceptúa el art. 284.1 LECrim. Es precisamente esa «participación», que podría efectuarse en términos genéricos pero suficientemente expresivos, la que permitiría a la fiscalía, a través de nuestros servicios territoriales, hacer uso de la facultad que contempla el artículo 284.2 c) de reclamar aquellos atestados que no habiendo sido remitidos al órgano judicial se estima, no obstante, deben dar lugar a la incoación del correspondiente procedimiento judicial y/o diligencias de investigación del Ministerio Fiscal.

De hecho, esa participación se ha llevado a efecto en algunos territorios, como por ejemplo en Valencia, dando lugar a que en el servicio de criminalidad informática de esa fiscalía se hayan incoado en el año un total de 189 diligencias de investigación justamente para valorar, haciendo uso de esa facultad, las posibilidades de prosecución de la

investigación del hecho denunciado en supuestos considerados como de autor desconocido por las unidades policiales.

Se hace necesario, a nuestro entender, adoptar decisiones en orden a una correcta interpretación y aplicación del nuevo art. 284 LECrim. A esos efectos pueden ser de utilidad los datos que aportamos en esta Memoria y que reflejan los atestados remitidos efectivamente a las autoridades judiciales. No obstante ha de tenerse en cuenta, a efectos de la correcta interpretación de la información que ofrecemos, que la diferencia de criterio –en los distintos cuerpos policiales o incluso en las diversas unidades territoriales de un mismo cuerpo policial– acerca de lo que ha de entenderse por autor desconocido ha determinado variaciones importantes en el porcentaje de atestados que finalmente han sido remitidos a las autoridades en cada uno de los diversos lugares de la geografía nacional.

Como ya hemos adelantado en el año 2016, el Ministerio Fiscal ha tenido conocimiento de la incoación de un total de 8.035 procedimientos judiciales por hechos delictivos competencia del área de especialidad cuyo detalle se especifica en la siguiente tabla:

Delitos informáticos		Procedimientos judiciales incoados	%
Delitos contra la libertad	Amenazas/coacciones cometidos a través de fas TICS (art. 169 y ss y 172 y ss)	989	12,31
	Acoso cometido a través de las TICs (art. 172 ter)	131	1,63
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	69	0,86
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	681	8,48
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	98	1,22
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	76	0,95
Delitos contra la intimidad	Ataques a sistemas informáticos/ interceptación transmisión datos (arts. 197 bis y ter)	115	1,43
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	404	5,03
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICS (art. 215)	100	1,24

Delitos informáticos		Procedimientos judiciales incoados	%
Delitos contra el patrimonio	Estafa cometida a través de las TICs (arts. 248 y 249)	4.930	61,36
	Descubrimiento de secretos empresariales (arts. 278 y ss)	49	0.61
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	16	0,20
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	114	1,42
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss)	54	0,67
Delitos de falsedad	Falsificación a través de las TICS	99	1,23
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICS (art. 510)	72	0,90
Otros		38	0,47
Total		8.035	100,00

Del análisis de los resultados estadísticos que ofrecemos se concluye claramente que el volumen más elevado de procedimientos judiciales registrados es el de los correspondientes a la investigación y enjuiciamiento de conductas delictivas englobadas genéricamente en los delitos de estafa, que sumaron 4.930, lo que supone un porcentaje del 61,36 % del total de incoaciones. Aun cuando este índice porcentual puede considerarse muy elevado, es interesante reseñar que ha experimentado un brusco descenso respecto de periodos anuales precedentes pues, en 2015, los procedimientos incoados por estos ilícitos supusieron un 80,62 % del total por ciberdelitos registrado en dicho periodo, porcentaje que supero el 84 % en 2014. Ello es debido a la importante disminución del volumen de incoaciones por procedimientos relacionados con actividades de carácter defraudatorio que se han reducido en un 72,91 % en comparación con los 18.201 registros del año 2015.

Todos estos datos sirven para constar que el índice mayor de atestados que finalmente no son trasladados a los órganos judiciales o al Ministerio Fiscal por parte de los cuerpos policiales tienen por objeto investigaciones relativas a ilícitos de esta naturaleza. Así, la comparación de las cifras absolutas obtenidas en el año memorial con las del periodo precedente no puede ser más clarificadora: el descenso en el número de procedimientos judiciales incoados entre los años 2015 y

2016 por hechos ilícitos de cualquier tipo competencia del área de especialidad se cifra, según nuestros datos, en 14.540 expedientes de los cuales, la diferencia mayor la ofrecen los correspondientes a delitos de estafa que se reducen en un montante de 13.271.

El hecho de que no se haya «participado» al Ministerio Fiscal información relativa a la mayoría de los atestados que finalmente no son trasladados a las autoridades de la jurisdicción penal, hace difícil que nos podamos pronunciar sobre la naturaleza y circunstancias de estas infracciones que aun siendo denunciadas no dieron lugar a procedimiento judicial. No obstante, contamos con algunas referencias correspondientes a territorios en los que se ha hecho llegar esta información a nuestros servicios de criminalidad informática y en base a ello podemos indicar que un número muy importante de dichos asuntos tuvieron por objeto actividades relacionadas con el uso fraudulento de tarjetas de crédito planificadas y/o ejecutadas bien sea físicamente desde el extranjero o mediante operaciones *on-line* y también es significativo el volumen de las que se refieren a ventas u ofrecimientos fraudulentos a través de la red cuya escasa cuantía ha llevado a considerar no justificada la práctica de diligencias de investigación que pudieran considerarse invasivas de derechos fundamentales. No obstante, ha de recordarse que muchas de esas denuncias lo que reflejan son efectos aislados de una misma actividad criminal, en la que han podido verse afectados un número importante de ciudadanos y en la que el montante global del perjuicio causado puede llegar a ser extraordinariamente elevado. Las disfunciones en el tratamiento y análisis conjunto de todas estas denuncias podrían determinar un cierto nivel de impunidad de esta clase de actividades delictivas y, en definitiva, la falta de respuesta del Estado de Derecho ante unos comportamientos que se están viendo generalizados como consecuencia de la utilización masiva de las tecnologías en las relaciones comerciales.

Centrándonos en los 4.930 procedimientos efectivamente incoados, la primera precisión que hemos de hacer, al igual que en años precedentes, es recordar que en este apartado se incluyen una diversidad de conductas encuadrables todas ellas en el art. 248 CP, pero que responden a dinámicas delictivas muy diferentes y, en consecuencia, presentan también problemáticas distintas en su investigación y en las posibilidades de actuación frente a sus responsables. Así incluimos en este apartado los expedientes por estafas de carácter más tradicional pero cuyos efectos se multiplican extraordinariamente como consecuencia del uso de las TIC en el planteamiento y desarrollo de la actividad criminal. Se trata de las ventas u ofrecimientos engañosos de bienes y servicios a través de la red, que cada año generan un número

importante de perjudicados y que abarcan todo tipo de productos: vehículos, pequeños electrodomésticos, dispositivos móviles o efectos informáticos y, cada vez con más frecuencia, ofertas de viaje y operaciones relacionadas con el mercado inmobiliario.

Ya hemos comentado en otras memorias el esfuerzo que está realizando el Ministerio Fiscal para reunir en un único procedimiento las múltiples denuncias que se presentan por los perjudicados por este tipo de acciones, normalmente dispersas por todo el territorio nacional, recabando para ello, desde la Unidad Central del área de especialización, la información oportuna de los Delegados territoriales y también de las unidades de investigación tecnológica de los cuerpos policiales. Nuestro objetivo es el de evitar la impunidad que pudiera derivarse de un análisis aislado de cada uno de los diversos efectos de estas actuaciones criminales y también solventar las posibles cuestiones de competencia que, con demasiada frecuencia, se generan en este tipo de asuntos. Dicho esfuerzo se ha concretado, en el año 2016, en la incoación de 29 expedientes de coordinación a través de los cuales hemos canalizado toda la labor de localización de procedimientos derivados de una misma actividad delictiva y acumulación de los mismos ante el órgano judicial competente. Se trata de una actuación laboriosa y de discreto resultado pero, a nuestro entender, importante para evitar la impunidad de estafas, a veces de escasa cuantía, en lo que se refiere al daño causado a cada uno de los perjudicados aisladamente considerados, pero en las que se ven afectados un número muy importante de ciudadanos y que generan pingües beneficios a sus autores, generalmente integrados en organizaciones o grupos criminales.

Otra modalidad reseñable de actividades ilícitas encuadrables en este mismo apartado son las transferencias económicas no consentidas que se llevan a efecto captando las claves bancarias de los perjudicados bien sea por técnicas de ingeniería social como en el caso del *phising* o mediante manipulaciones informáticas como en los supuestos, cada vez más frecuentes, en los que un previo ataque informático, bien sea de interceptación de comunicaciones o de acceso ilegal a un sistema, permite a los delincuentes hacer suya información de esa naturaleza que posteriormente es utilizada para ordenar traspasos de dinero u otras operaciones comerciales en beneficio propio. Sin embargo la variante que, según informan muchos de los Delegados provinciales –Cantabria, Teruel o Vizcaya, entre otros–, se está produciendo con más frecuencia es la relacionada con el uso irregular de tarjetas de crédito o débito o de sus datos, *carding,* ya sea previa sustracción de la tarjeta física o por la captación no autorizada de sus

datos, supuestos que, como hemos indicado y por las razones expuestas, en muchos casos no dan lugar ni tan siquiera a la incoación de actuaciones judiciales, aun cuando generan un importantísimo volumen de movimientos económicos de carácter fraudulento cuya cuantía total difícilmente puede ser precisada.

Antes de dar por concluido el análisis de estas figuras hemos de hacer referencia también a las defraudaciones vinculadas con el juego *online* y también a las que se asocian a la utilización irregular de los servicios de telecomunicaciones; así junto a las ya más tradicionales de contratación irregular o de suscripción no consentida a servicios de tarificación adicional, se va detectando la utilización de dinámicas de carácter más técnico como las relacionadas con el cambio de números de serie o la alteración en el by-pass internacional, que están generando gravísimos perjuicios económicos a las operadoras de comunicaciones.

Otras tipologías delictivas de especial interés a estos efectos son las que sancionan los ataques a los sistemas de información que sumaron 682 registros en el año 2016, un 8,48 % del total de las incoaciones anuales por hechos ilícitos vinculados al uso de las TIC. Incluimos en este capítulo los ataques que podríamos definir como de espionaje informático, susceptibles de calificarse bien sea como delitos de descubrimiento y revelación de secretos de particulares y/ o de empresas (arts. 197 y 278 y siguientes del Código Penal) o como accesos ilegales o interceptación no autorizada de comunicaciones entre sistemas (art 197 bis) y también los encuadrables en la categoría de daños informáticos (art. 264, 264 bis y 264 ter). En la evolución interanual de los expedientes judiciales incoados por este tipo de acciones se ha dejado sentir también los efectos del nuevo régimen de traslado de atestados a los órganos de la jurisdicción penal. Así, los relacionados con espionaje informático, analizados conjuntamente, dieron lugar en el año 2016 a la incoación de 568 causas, un 48 % menos que en el año 2015 en el que se alcanzó la cifra de 1.093 registros por iguales conceptos. Por su parte los procedimientos por daños informáticos en sus diversas manifestaciones, que sumaron 114 registros, acusan un descenso del 61 % respecto de la anualidad precedente. Integrando los resultados de todas las figuras penales en que se sancionan ataques informáticos, el índice de descenso se cifra en un 50,86 % al evolucionar a la baja desde los 1.388 registros del año 2015 a los 682 del año memorial.

También en este caso, los resultados obtenidos se explican fácilmente por la no remisión a las autoridades de la jurisdicción penal de aquellos atestados en los que se entiende no es posible la determina-

ción de su autor. Por ello y sin perjuicio de dar por reproducidos los razonamientos anteriormente expuestos sobre la posibilidad de rastrear las huellas tecnológicas que necesariamente suelen dejar este tipo de agresiones informáticas, hemos de llamar la atención acerca de la importancia que tiene conocer, con la mayor precisión posible, la frecuencia, incidencia e intensidad de este tipo de acciones para estar en condiciones de poder articular las medidas necesarias para hacer frente a estos comportamientos que pueden llegar a afectar muy seriamente a ciudadanos, empresas, entidades públicas y/o privadas e, incluso, a las infraestructuras críticas. Ciertamente dicho objetivo, al menos en los aspectos de carácter preventivo, puede ser atendido en muy buena medida con las obligaciones de notificación de incidentes que se generarán a resultas de la incorporación al ordenamiento jurídico interno de la Directiva NIS antes mencionada, pero la posibilidad de actuación penal frente a estas conductas, con sus efectos derivados de prevención general y especial, tiene también un valor no desdeñable. Por ello es importante no descuidar la posibilidad de efectuar un seguimiento adecuado de la evolución de esas manifestaciones criminales para estar en condiciones de poder articular las medidas de carácter penal, procesal u operativo que se estimen necesarias para evitar la impunidad de dichos comportamientos.

En la memoria son, sin duda, una referencia obligada los delitos que se sirven de las TIC para atentar contra la libertad e indemnidad sexual y, en particular aquellos relacionados con pornografía infantil o de personas con discapacidad o con el *child grooming*. La preocupación que generan este tipo de acciones transciende, desde hace años, nuestro ámbito geográfico alcanzando una dimensión internacional que ha dado lugar a la publicación de una diversidad de Tratados y Convenciones Internacionales sobre esta materia y también a una eficaz colaboración internacional en la investigación y persecución penal de estas conductas. Esta preocupación se justifica, sin duda, por la importancia de los bienes jurídicos afectados y por la peligrosa incidencia que el vertiginoso desarrollo tecnológico está teniendo en la planificación y desenvolvimiento de estas criminales conductas y en la difusión de dichos contenidos.

Los delitos de pornografía infantil registran, en el último periodo anual, un leve descenso en el volumen de incoaciones que se cifra en un 11,21 % respecto de los 767 expedientes detectados en el año 2015. A diferencia de lo que venimos comentando en referencia a otros tipos penales, dicho resultado no ha de imputarse, en este caso, al nuevo régimen de traslado de atestados a las autoridades judiciales dado que según el texto vigente del art. 284.2a) LECrim, estas tipologías delic-

tivas constituyen una de las excepciones a la regla general antes mencionada, por lo que la falta de datos acerca del autor no implica que las actuaciones no lleguen a conocimiento de los órganos judiciales y/o del Ministerio Fiscal. Como tampoco esta reducción en el volumen de procedimientos puede llevar a pensar en un descenso en las acciones criminales de este tipo que, por contra y como indicábamos, se han visto impulsadas por las capacidades que ofrecen las nuevas herramientas tecnológicas. La leve disminución detectada no es sino una variación intrascendente en un tipo de investigaciones cuya evolución suele depender, no tanto de la denuncia de perjudicados, sino de la actuación de oficio de unidades policiales especializadas a partir de la información que localizan en sus actividades de ciberpatrullaje en fuentes abiertas o por comunicación de autoridades de otros países y también de entidades prestadoras de servicios o, incluso, de usuarios particulares que, con ocasión de su navegación por la red, detectan dichos contenidos ilícitos vinculados a direcciones IP inicialmente de origen español.

No obstante, las investigaciones en curso por delitos de pornografía, aunque un poco menos frecuentes, ofrecen como característica una dificultad cada vez mayor. Así junto a los supuestos más tradicionales en nuestro país, centrados básicamente en actividades de distribución y posesión –para propio consumo o preordenada al tráfico– se están detectando, en los últimos años, otros de naturaleza más grave y compleja en las que el material pornográfico se elabora directamente en el territorio nacional, organizándose también desde aquí la posterior distribución del mismo. Las capacidades que ofrecen las nuevas tecnologías están facilitando a los depredadores sexuales la preparación de este material mediante la grabación y posterior tratamiento de los actos de agresión y abuso sexual a menores, que ellos mismos ejecutan o hacen ejecutar a otros, bien sea físicamente o a través de contactos *on-line*. Se trata por tanto de actividades, planificadas y ejecutadas, individualmente o por grupos organizados, en las que concurren diversas figuras delictivas, por lo que su investigación presenta mayores dificultades y en ocasiones exige la utilización de herramientas tecnológicas novedosas como las operaciones encubiertas *on-line*, técnica cuya incorporación específica a nuestra legislación tiene su origen en la última reforma procesal.

Por su parte, los delitos de *child grooming*, dieron lugar en 2016 a un número de registros exactamente igual al del año precedente, cifrado en 98 causas judiciales. Ha de recordarse que, al tratarse de hechos ilícitos que atentan contra la libertad e indemnidad sexual, se

enmarcan en la excepción prevista en el art. 284.2a) LECrim, antes comentada, por lo que estos resultados no se han visto afectados por el nuevo régimen de traslado de expedientes a las autoridades judiciales establecido en dicho precepto. En cualquier caso, es interesante recordar que muchas de estas conductas están dirigidas a la obtención de material pornográfico de menores de 16 años, por lo que no es infrecuente que aparezcan en concurso con los delitos anteriormente comentados y en consecuencia confundidos con ellos, en su cómputo estadístico.

Consideración independiente merecen también las conductas cometidas a través de las TIC que afectan a derechos personalísimos como la libertad y seguridad de las personas. Incluimos aquí los comportamientos susceptibles de tipificarse como delitos de amenazas y/o coacciones y también los de acoso permanente encuadrables en el art. 172 ter 1.º n.º 2 CP. Esta clase de conductas dieron lugar en 2016 a 1.120 incoaciones, casi un 14 % del total de los registros anuales, lo que supone un levísimo ascenso, de poco más del 1 % respecto de las 1.105 causas computadas en 2015 en este apartado. El análisis más detallado de estas cifras revela que el incremento más importante se ha producido en referencia a los delitos de acoso permanente que ascienden desde los 96 expedientes del año 2015 a los 131 del presente año, dato que se explica fácilmente si se tiene en cuenta que el citado precepto (de nueva planta en nuestro código penal) se encuentra vigente desde el 1 de julio del año 2015 por lo que dichas conductas, hasta ese momento, se venían tipificado en las figuras genéricas de amenazas o coacciones cuando concurrían los requisitos necesarios para ello.

La utilización de las TIC para llevar a efecto estas conductas contra las personas ofrece una clarísima evolución al alza de la que dan cuenta, no solamente varios de los Delegados Provinciales, como los de Granada, Jaén, Santa Cruz de Tenerife, Guipúzcoa o Albacete, entre otros, sino también el análisis de los resultados obtenidos en comparación con los años precedentes. Así, los 249 registros del año 2013 ascendieron a 527 en 2014, para elevarse hasta las cifras de 1105 y 1120 antes indicadas en los últimos años. Tanto es así, que ni siquiera la modificación del art. 284.2 LECrim parece haber tenido una incidencia efectiva en los registros judiciales relativos a estos delitos, circunstancia que también se explica porque se trata de conductas en las que, por su propia naturaleza, la identidad del autor suele ser conocida o fácilmente determinable, incluso por medios o fuentes de prueba ajenos a las herramientas tecnológicas.

El uso generalizado de las TIC por los ciudadanos está determinando que los nuevos medios de comunicación (correo electrónico, mensajería instantánea *(whatsapp, telegram)*, mensajes de voz o SMS, comunicación a través de redes sociales, etc.) se hayan convertido en cauce habitual para que los agresores trasladen fácilmente toda clase de amenazas y actos de coacción o persecución a sus víctimas y también para canalizar el hostigamiento o persecución constante y permanente hacia ellas. Por ello no es infrecuente encontrar este tipo de conductas asociadas a problemas de relación entre menores de edad o a situaciones de violencia de género o intrafamiliar. Tanto es así que el Comité Permanente de la Convención de Budapest contra la Ciberdelincuencia del Consejo de Europa ha promovido una iniciativa para extender el ámbito de aplicación de dicho Convenio a los supuestos de violencia sobre mujeres o niños cometidos a través de estas tecnologías.

Muy vinculados a este tipo de acciones son aquellas otras que atentan contra la integridad moral de las personas, que dieron lugar en el año 2016 a 69 registros frente a los 226 del año 2015, lo que supone un descenso interanual del 69,46 %. Sin embargo, este dato ha de valorarse cuidadosamente pues bien pudiera ser debido, como sugiere la Fiscal Delegada de Madrid, a que muchas de las conductas que desde la fiscalía se venían enmarcando en el art. 173.1 CP, encuentran actualmente su acomodo en el artículo 197.7 del mismo texto legal, precepto en el que, tras la última reforma de la norma penal sustantiva, se sanciona la difusión no consentida de imágenes de carácter íntimo.

También en los delitos contra la propiedad intelectual se detecta un descenso notable en el volumen de procedimientos incoados en el año, pues se reducen desde los 70 del año 2015 a los 54 del 2016, rompiéndose de esta forma la tendencia alcista que se venía observando en años precedentes. Son procedimientos, no obstante, que son objeto de un especial seguimiento y atención por parte de la fiscalía dado el perjuicio económico que generan a los titulares de derechos protegidos y la circunstancia de que, generalmente, ofrecen significativas dificultades en su investigación y enjuiciamiento aunque ha de reconocerse que la nueva redacción dada a los artículos 270 y siguientes del Código Penal ha solventado en buena medida dichas dificultades.

Como ya es tradicional, los delitos de odio son también objeto de específica mención en esta memoria, aunque ciertamente es esta una materia cuyo conocimiento ha sido asignado a un área específica de

actuación del Ministerio Fiscal. La circunstancia de que una buena parte de esas actividades ilícitas se sirvan de las TIC en su planificación y ejecución y la coincidencia, en muchos territorios, de ambas áreas de especialización en una misma sección de la fiscalía, determina que sea esta una materia que no pueda ser obviada al analizar la problemática asociada a la criminalidad informática. De hecho una buena parte de las Diligencias de Investigación incoadas en el año 2016 por nuestra Unidad Central ha tenido por objeto determinar, mediante una investigación puramente tecnológica, el origen de contenidos denunciados como crímenes de odio, para posteriormente dar traslado de esa información al área de Tutela Penal de la Igualdad y contra la Discriminación a efectos de la oportuna valoración acerca de la concurrencia de los elementos que exige la aplicación de dichos tipos penales.

A diferencia de los resultados obtenidos en referencia a la generalidad de las figuras delictivas, los crímenes de odio cometidos a través de las TIC han dado lugar a un incremento importante en el número de procedimientos incoados en 2016, al evolucionar desde los 40 expedientes registrados en 2015 a los 99 del presente año, lo que supone un índice al alza de algo más del 147 %. Este aumento, motivado sin duda por una mayor sensibilización social frente a los actos de discriminación, violencia o desprecio frente a determinados colectivos especialmente vulnerables, no se ha visto afectado por el nuevo régimen de traslado de atestados a los órganos de la jurisdicción penal porque un número importante de las denuncias relativas a la difusión de contenidos ilícitos encuadrables, en principio, en el discurso del odio se presentan directamente ante el Ministerio Fiscal por los propios perjudicados o por asociaciones preocupadas por defender los intereses de las víctimas. Es más, incluso no es infrecuente, que estos procedimientos tengan su origen en actuaciones que realiza de oficio la Fiscalía al llegar a su conocimiento conductas de esta naturaleza, como consecuencia derivada del claro compromiso asumido por la Institución frente a estos reprobables comportamientos.

8.2.1 Acusaciones del Ministerio Fiscal

Durante el año 2016, la Fiscalía española presentó un total de 1.648 escritos de acusación por hechos ilícitos competencia del área de especialización en criminalidad informática. Esta cifra supone un

importante incremento, cuantificado en un 32,68 % respecto del año precedente, en que dicha cifra fue de 1.242. Se retoma así la tendencia ascendente que venimos constatando, con la excepción del citado año 2015 en que detectamos un ligero descenso de poco más del 2 %, desde el inicio de la constitución de la red, en el año 2011, anualidad en la que registramos un total de 906 escritos de esa naturaleza. Quiere decirse con ello, que con independencia de que se haya reducido de forma muy notable el número de procedimientos judiciales incoados por hechos ilícitos vinculados al uso de las TIC, la capacidad de concretar las investigaciones en acusaciones específicas contra personas perfectamente determinadas y por tanto de ofrecer una respuesta adecuada desde el Estado de Derecho frente a estas conductas va mejorando progresivamente.

El detalle de las acusaciones formuladas en atención a las distintas tipologías delictivas, es el siguiente:

Delitos informáticos		Calificaciones	%
Delitos contra la libertad	Amenazas/coacciones cometidos a través de las TICs (art. 169 ss y 172 y ss)	242	14,68
	Acoso cometido a través de las TICs (art. 172 ter)	23	1,40
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	36	2,18
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	332	20,15
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	38	2,31
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	22	1,33
Delitos contra la intimidad	Ataques a sistemas informáticos/ interceptación transmisión datos (arts. 197 bis y ter)	26	1,58
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	107	6,49
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICs (art. 215)	30	1,82

Delitos informáticos		Calificaciones	%
Delitos contra el patrimonio	Estafa cometida a través de las TICs (art. 248 y 249)	633	38,41
	Descubrimiento de secretos empresariales (art. 278 y ss)	16	0,97
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	20	1,21
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	22	1,33
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss)	32	1,94
Delitos de falsedad	Falsificación a través de las TICs	45	2,73
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	13	0,79
Otros		11	0,67
Total		1.648	100,00

Como se constata claramente el volumen más importante de acusaciones se corresponde con delitos de estafa que suponen un 38,41 % del total de las formuladas durante el año 2016. En este apartado se incluyen las relativas a cualquier tipología delictiva de las sancionadas en el art. 248 CP que hayan sido planificadas y/o ejecutadas a través de las TIC. Por tanto se incluyen tanto las formuladas por ventas u ofrecimientos de servicios engañosos, defraudaciones por *phising* (dirigidas normalmente contra quienes ejerciendo como mulas intervienen en la recogida de dinero y su envío a los responsables de la organización criminal), uso indebido de tarjetas de crédito o débito, etcétera, sin que por el momento nuestras aplicaciones informáticas nos permitan, como sería deseable, ofrecer datos más específicos en referencia a cada una de esas actividades criminales.

El volumen de acusaciones por estas tipologías delictivas se ha incrementado en mas de un 24 % en relación con las formuladas en el año precedente, lo que supone romper la tendencia descendente de la que veníamos dando cuenta en anteriores memorias desde el año 2013, pues las 618 acusaciones presentadas por estos ilícitos en el indicado periodo anual, se redujeron a 577 en 2014 y a 508 en 2015, recuperándose, por tanto, en el año memorial índices que no registrábamos desde hace tiempo.

Le siguen en importancia las acusaciones formuladas por delitos de pornografía infantil o de personas con discapacidad, que se elevaron a 332, un 20,15 % del total de las presentadas. También en este caso

detectamos un cambio claro de tendencia, dado que en el año 2015, los escritos presentados fueron 251 frente a los 285 del año 2014. Esta circunstancia sirve para constatar una evidente mejora en la eficacia frente a este tipo de actividades ilícitas. Llama la atención que el número de acusaciones formuladas –332– casi llegue a la mitad del de los procedimientos judiciales incoados en el año por estos mismos delitos, que ascienden a 681, proporción que da cuenta de unos resultados extraordinariamente positivos en lo que se refiere a la capacidad para concretar las investigaciones en hechos y personas determinadas. Aunque la comparación no pueda plantearse en términos exactos porque muchos de los escritos de calificación se corresponden con procedimientos incoados en otros periodos anuales, la coincidencia de una proporción muy similar en anteriores memorias avala dicho resultado, que en buena parte es debido a las propias características de las investigaciones que se suelen iniciar a partir del conocimiento policial de direcciones IP desde las que se opera con el ilícito material. También es llamativo, en este tipo de asuntos, el elevado porcentaje de sentencias dictadas de conformidad, dado que el acusado prefiere aceptar la condena a verse sometido a un juicio público en el que su conducta llegue a ser conocida por sus conciudadanos.

Como ya hemos indicado, en los últimos meses estamos viendo evolucionar la dinámica de las actividades ilícitas que son objeto de enjuiciamiento en este ámbito. Junto a las más tradicionales conductas que se concretan en la distribución o posesión de pornografía, se empiezan a enjuiciar acciones en las que el imputado ha fabricado/elaborado por sí mismo, bien individualmente o bien actuando en grupo, el material pornográfico que luego distribuye. Muchos de estos comportamientos están asociados a otras figuras delictivas como aquellas que implican agresiones o abusos físicos a menores o personas con discapacidad o las encuadrables en el tipo penal que sanciona el *child grooming* en el art. 183 ter CP, lo que puede distorsionar en cierta medida los resultados estadísticos que ofrecemos.

Precisamente en referencia a este último tipo penal detectamos también un incremento de más de un 65 % en el volumen de acusaciones presentadas respecto del año 2015 y una proporción también bastante elevada entre el número de procedimientos incoados, 98, y el de acusaciones formuladas, 38. La más que justificada preocupación por este tipo de conductas determina un especial esfuerzo en el esclarecimiento de estos hechos y la determinación de sus autores, lo que sin embargo no impide que exista una cifra oculta de criminalidad en este ámbito que ha de hacerse aflorar. A ello, sin duda, contribuirán las campañas de sensibilización social en las que ya se está trabajando,

especialmente en el entorno educativo de los menores, y en las que la Fiscalía está colaborando, en la medida de sus posibilidades, en los distintos territorios.

Otra materia en la que es llamativo el incremento en el volumen de escritos de acusación presentados es el correspondiente a los delitos contra la libertad y seguridad de las personas, en los que incluimos los relativos a amenazas y coacciones y los formulados en base a la nueva figura del acoso permanente sancionada en el art. 172 ter CP. En este apartado hemos evolucionado desde los 137 escritos de acusación de 2015 a los 265 del año memorial, es decir, un incremento conjunto del 93,43 %, que analizado en detalle desvela que las acusaciones por delitos de amenazas y coacciones han crecido en casi un 82 % en tanto que las correspondientes al delito de acoso permanente lo han hecho en un 475 %. Aun cuando ha de reconocerse que este último dato es fácilmente explicable por que el tipo penal del art. 172 ter, solo es aplicable a las conductas cometidas después del 1 de julio del año 2015, es evidente que, como indicamos en anteriores apartados de esta misma memoria, la incidencia del uso de las tecnologías en este tipo de acciones criminales es cada vez más importante y no ha de ser descuidada en cualquier planteamiento serio de política criminal.

A estos efectos la evolución interanual de las acusaciones por este tipo de conductas no puede resultar más clarificadora. Así, las 29 y 27 acusaciones por delitos contra la libertad y seguridad a través de las TIC que, respectivamente registramos en los años 2011 y 2012, sumaron 55 en la estadística correspondiente al año 2013, para elevarse a 93 en 2014 y alcanzar las cifras de 137 y 265, respectivamente en los dos últimos años.

Las acusaciones formuladas en las tipologías delictivas asociadas a los ataques informáticos han tenido también en el año 2016 un crecimiento significativo, del 42,5 %, si comparamos las 120 acusaciones presentadas, en conjunto, por esos delitos en 2015 con las 171 elaboradas en el año memorial. El incremento más significativo lo ofrecen en esta materia los delitos de descubrimiento y revelación de secretos de particulares que han dado lugar a un aumento en un 48,6 % en el volumen de acusaciones registradas en el año 2016 hasta alcanzar la cifra de 107. No obstante, reiteramos que es esta una materia en la que ha de incentivarse el esfuerzo por parte de investigadores y órganos de la jurisdicción penal, dada la cifra oculta de criminalidad en este ámbito y el riesgo que entrañan este tipo de acciones para el normal funcionamiento de los sistemas informáticos en los que se apoya la actividad ordinaria de instituciones, empresas y entidades de todo tipo y también las relaciones políticas, económicas y sociales, en las que todos nos encontramos de una u otra forma implicados.

8.2.2 Diligencias de investigación del Ministerio Fiscal

Terminamos el análisis de los datos estadísticos del año 2016, con la información sobre estos expedientes, incoados y tramitados en el seno de la propia Institución al amparo del artículo 5 de nuestro Estatuto Orgánico y 773-2 de la Ley de Enjuiciamiento Criminal. Se trata de expedientes iniciados por la Fiscalía, ya sea de oficio o por denuncia de particulares, colectivos o incluso de otras instituciones públicas, en los que el Ministerio Fiscal lleva a efecto su propia investigación acerca la actividad delictiva y de sus autores, dando posteriormente traslado al órgano judicial competente para la prosecución del procedimiento, si existen méritos suficientes para ello, o acordando, en caso contrario, el archivo de las actuaciones. Obviamente el marco de la actividad que desarrollamos en estas diligencias preprocesales queda definido por nuestra propia capacidad de actuación por lo que, en consecuencia, el Fiscal ha de acudir necesariamente al órgano judicial tan pronto como sea necesario llevar a efecto actividades que incidan en derechos fundamentales y precisen de la autorización del Juez de Instrucción.

Como se ha indicado en memorias precedentes, en esta área de especialización, el recurso a este tipo de expedientes se encuentra muy limitado precisamente porque la identificación y seguimiento de las huellas o del rastro que dejan muchos de los ilícitos cometidos a través de las TIC compromete derechos fundamentales y por tanto resulta necesario recabar la autorización del órgano judicial correspondiente. Por ello, las cifras que anualmente ofrecemos acerca de estas diligencias de investigación penal suele ser bastante reducida.

En estas circunstancias, sorprende el incremento en más de un 232 % en el número de las incoadas en el año 2016, respecto del año 2015 en el que se incoaron 95 de estas diligencias. Este resultado es debido, también en este caso, al nuevo régimen establecido en el art. 284 LECrim, para el traslado de los atestados a los órganos de la jurisdicción penal. Como ya indicamos al inicio de esta memoria, en algunos territorios, los cuerpos policiales han seguido informando al Fiscal Delegado de criminalidad Informática de todos los atestados que iniciaban, incluidos aquellos de los que posteriormente no daban traslado a las autoridades judiciales por entender no había autor conocido. Pues bien, como quiera que en algunos de estos últimos la fiscalía ha entendido que el autor podía ser localizado, se ha procedido por nuestra parte, al amparo del citado art. 284.2 c) a iniciar diligencias de investigación para la práctica de las actuaciones necesarias para ello, remitiendo posteriormente las mismas al órgano

judicial o acordando su archivo, si así se entendiera procedente. Este factor, completamente novedoso es el que determina la importante variación en el volumen de expedientes de esta naturaleza, cuyo detalle es el siguiente:

Delitos informáticos		Diligencias investigación	%
Delitos contra la libertad	Amenazas/coacciones cometidos a través de las TICs (art. 169 y ss y 172 y ss)	23	7,28
	Acoso cometido a través de las TICs (art. 172 ter)	0	0,00
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	3	0,95
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	3	0,95
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	5	1,58
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	3	0,95
Delitos contra la intimidad	Ataques a sistemas informáticos/ interceptación transmisión datos (arts. 197 bis y ter)	11	3,48
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	20	6,33
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICs (art. 215)	8	2,53
Delitos contra el patrimonio	Estafa cometida a través de las TICs (art. 248 y 249)	144	45,57
	Descubrimiento de secretos empresariales (art. 278 y ss)	1	0,32
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	1	0,32
	Delitos de daños informáticos (arts 264, 264 bis y 264 ter)	8	2,53
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss)	2	0,63
Delitos de falsedad	Falsificación a través de las TICs	2	0,63
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	82	25,95
Otros		0	0,00
Total		316	100,00

Como puede constatarse y por las razones expuestas, el volumen más elevado corresponde a las incoadas por delitos de estafa, un 45,5 %, dato que se deriva del hecho, ya comentado, de que buena parte de los atestados que finalmente no son remitidos a los órganos judiciales tienen por objeto la investigación de hechos ilícitos de esta naturaleza, siendo por tanto estas investigaciones las que determinan con mayor asiduidad la reclamación del atestado por parte del Fiscal para dar continuidad a la investigación policial.

Le siguen en importancia las diligencias relativas a delitos de odio que ascienden a 82, integrando casi un 26 % del total de las incoadas, dato que confirma, además, la tendencia alcista detectada desde hace varios años. Así hemos pasado de los 10 expedientes abiertos por estos ilícitos en 2013, a los 23 del 2014, 50 del 2015, hasta alcanzar la cifra indicada en el año memorial. También en este caso, los resultados obtenidos avalan las reflexiones anteriormente efectuadas. El empeño del Ministerio Fiscal en la protección de los colectivos especialmente vulnerables está determinando que la Institución se haya convertido en receptora de muchas de las denuncias que se presentan por la difusión a través de las TIC de contenidos de esta naturaleza, realizándose por nuestra parte, antes de la judicialización del expediente, cuantas actuaciones se consideran necesarias para la constatación de la veracidad de los hechos denunciados y la identificación de sus autores.

Igualmente se han de destacar por su relevancia, el volumen de diligencias abiertas por la Fiscalía en referencia a los supuestos de espionaje informático, delitos de los art. 197 y 197 bis CP y también respecto a delitos de amenazas y coacciones. En el primer caso, la cifra conjunta asciende a 31 expedientes y a 23 en las relativas a delitos contra la libertad y seguridad, lo que supone respectivamente porcentajes del 9,8 % y 7,28 % del total de incoaciones anuales.

8.3 **Relaciones con instituciones u organismos públicos y con las Fuerzas y Cuerpos de Seguridad**

En lo que concierne a las relaciones entre las secciones especializadas y las Fuerzas y Cuerpos de Seguridad, además de lo indicado al inicio de este capítulo dedicado a la actividad del área de especialización, cabe añadir que la generalidad de los Fiscales Delegados destacan la existencia de unas fluidas relaciones con las unidades policiales encargadas de las investigaciones tecnológicas que se concretan tanto en la celebración de reuniones para tratar los problemas técnico-jurí-

dicos surgidos en el curso de las mismas, como en la comunicación al Fiscal Delegado de toda la información relevante sobre asuntos de especial interés.

Por lo que respecta a la Unidad Central hemos de resaltar que el funcionamiento de nuestras unidades de enlace con el Cuerpo Nacional de Policía y la Guardia Civil, ubicadas en la propia sede de Fiscalía, está plenamente consolidado y su actuación no solo resulta esencial para el desarrollo de las labores de coordinación asignadas a éste área de especialización sino que constituye la correa de transmisión entre una y otras instituciones, convirtiéndose en factor decisivo para obtener un conocimiento permanente y actualizado de las investigaciones tecnológicas de especial relevancia y para facilitar la comunicación fluida con los grupos policiales especializados con el fin de establecer líneas de actuación que contribuyan al éxito de las mismas.

En el año memorial, como en anteriores ejercicios, la Unidad Central ha mantenido frecuentes contactos con aquellos organismos e instituciones que por razón de sus competencias se encuentran implicados en la lucha contra la ciberdelincuencia, tal es el caso de los Ministerios de Justicia y de Educación, Cultura y Deporte, el Centro Nacional de Protección de Infraestructuras Criticas (CNPIC), dependiente del Ministerio del Interior, el Embajador en Misión Especial en materia de Ciberseguridad, el Instituto Nacional de Ciberseguridad (INCIBE), el Consejo General de la Abogacía o el Ilustre Colegio de Abogados de Madrid, entre otros. En la mayor parte de las ocasiones tales encuentros tuvieron por objeto el análisis y tratamiento de aspectos diversos de carácter técnico-jurídico relacionados con los ciberdelitos y su investigación. No obstante, en algunos casos, y en éste sentido merecen especial mención las relaciones con INCIBE, dichos contactos se han orientado a optimizar el funcionamiento del área de especialización aprovechando los recursos que tales Instituciones pueden ofrecer y/o a establecer vías de mutua cooperación en el ámbito formativo mediante la participación activa de los integrantes del área de especialización en actividades formativas y foros de debate de otras Instituciones y, viceversa.

Ha de mencionarse igualmente que, en septiembre de 2016, fijamos las bases de una línea de colaboración permanente, en asuntos de interés común, con la Agencia Española de Protección de Datos tras una sesión de trabajo conjunto, celebrada en la sede de dicho organismo, en la que participaron su Directora y miembros del Gabinete Jurídico y del Área de Inspección, y las fiscales integrantes de la Unidad Central del área de especialización. Dicha colaboración ha facili-

tado el traslado a la fiscalía de determinadas denuncias presentadas ante la Agencia y que por su contenido pudieran tener relevancia penal.

En el marco de las relaciones internacionales, se ha dado continuidad a la participación de la Fiscal de Sala Coordinadora, por designación expresa del Ministerio de Justicia, en las reuniones del TC-Y de la Convención de Budapest del Consejo de Europa, que tuvieron lugar los días 24 y 25 de mayo y 14 y 15 de noviembre, así como en la Conferencia Octopus, celebrada a continuación de la segunda de ellas, en la que la Fiscal de Sala intervino como ponente, en la sesión inaugural, para exponer la visión del Ministerio Fiscal en la lucha contra la ciberdelincuencia. En ambos casos y como es habitual, las conclusiones obtenidas en dichas reuniones fueron trasladas al Ministerio de Justicia.

También en el año memorial se puso en marcha la Red Judicial Europea de Cibercrimen (EJCN) impulsada por el Consejo de la Unión Europea para dar cumplimiento a sus conclusiones adoptadas el 9 de junio del mismo año, en las que se subrayaba la importancia de la cooperación internacional en la investigación de los ciberdelitos y en la obtención de evidencias tecnológicas y se abogaba por mejorar el intercambio de información entre autoridades judiciales y expertos a través de la creación de una red de expertos con el apoyo de Eurojust. A tal fin el Consejo de la UE instó a cada Estado miembro a designar al menos un representante nacional como punto de contacto de dicha red. En cumplimiento de lo acordado, el Ministerio de Justicia, con apoyo en lo establecido en el artículo 33 de la Ley 16/2015, de 7 de julio, acordó el nombramiento de tres puntos de contacto, en representación respectivamente del Poder Judicial; del Ministerio de Justicia y del Ministerio Fiscal, habiendo recaído esta última designación en la Ilma. Sra. doña Ana M.ª Martín Martín de la Escalera, en su calidad de Fiscal Adscrita a la Fiscal de Sala contra la Criminalidad informática.

El principal objetivo de la nueva Red es el de favorecer y mejorar la cooperación entre las autoridades judiciales competentes en esta materia, facilitando el intercambio de experiencias, buenas prácticas, y conocimientos especializados, así como fomentar el diálogo entre los principales actores involucrados en la lucha contra la ciberdelincuencia. El 24 de noviembre tuvo lugar la primera reunión plenaria de la Red en la que, además del estudio de determinados temas de especial relevancia como la encriptación de datos y la investigación encubierta *on-line*, se establecieron algunas de las futuras pautas de actuación de esta red y, concretamente, la elaboración de planes de trabajo bianuales; la realización de actividades a través de grupos de trabajo y la programación anual de reuniones y/o de sesiones cerradas

para temas concretos. Por último, en dicha reunión, se acordó también el nombramiento de una Junta informal (integrada por representantes del trío presidencial del Consejo de La Unión Europea y de Eurojust) con la función de impulsar el funcionamiento de la red.

Por último ha de recordarse la actividad que desarrolla el Grupo de Trabajo creado a nivel europeo para reforzar la actuación frente a los delitos contra la propiedad intelectual e industrial cometidos a través de estas tecnologías, de la que forman parte activa, la Fiscal Adscrita, Ilma. Sra. Doña Pilar Rodríguez Fernández y el Fiscal Delegado de Cádiz, Ilmo. Sr. Don Rafael Payá Aguirre.

8.4 **Estructura y funcionamiento del área de especialización. La Red de Fiscales especialistas en criminalidad informática**

Como ya se indicó en la memoria anterior, 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 supuesto la consolidación y fortalecimiento de la estructura organizativa ya existente en esta área de especialización, que integrando los puntos de contacto de las Fiscalías de área y los Fiscales colaboradores destinados en secciones territoriales o en otros servicios especializados, alcanza la cifra de 131 miembros, a los que han de sumarse las tres fiscales que componemos la Unidad Central. Desde la puesta en funcionamiento de la red, en los primeros meses del año 2012, ha sido claramente perceptible la evolución de una buena parte de las secciones provinciales en lo que a su composición, estructura interna y funciones asignadas se refiere, pues se ha ido incrementando año tras año el número de fiscales que las componen y, al tiempo, se han ampliado y potenciado las atribuciones que los respectivos Fiscales Jefes van otorgando a esas mismas secciones y/o a sus Delegados Provinciales. Así, si hace unos años la labor de los miembros de la red se limitaba exclusivamente al control de asuntos y a la resolución de consultas jurídicas que pudieran surgir en la investigación o enjuiciamiento de ciberdelitos, en la actualidad en muchas de las provincias, significativamente en las fiscalías más grandes, el Delegado y, en su caso, los restantes miembros de la Sección, asumen la intervención en la tramitación y enjuiciamiento de los asuntos competencia del área de especialidad e incluso el visado de escritos por delegación del Fiscal Jefe. Precisamente por considerarse ésta una buena práctica, sería aconsejable que esa labor de visado o, al menos, de revisión de los escritos de acusación con carácter previo al visado

definitivo por parte del Fiscal Jefe, fuera generalizándose en todos las órganos territoriales, pues facilitaría, sin duda, la unificación de criterios, en una materia especialmente compleja y sujeta continuamente a modificaciones legislativas

El incremento en el número de fiscales integrantes de la red de especialistas repercute necesariamente en el volumen de asuntos o cuestiones concretas que se trasladan a la Unidad Central, siempre con el objetivo último de asegurar una unidad de criterio en la interpretación y aplicación de las normas jurídicas. Así, son frecuentes las consultas acerca de la forma de abordar alguna concreta investigación y también sobre la aplicación de los tipos penales o de las medidas tecnológicas de investigación previstas en la LECrim, siendo merecedoras de especial atención, por su novedad y su alcance, las relativas a la utilización de la figura del agente encubierto informático y al registro remoto de sistemas informáticos.

Igualmente, en el último año, ha aumentado el número de escritos de acusación que se remiten a la Unidad Central para su supervisión, tal y como establece la Instrucción 1/2015 antes mencionada. Concretamente dicho tramite se lleva a efecto en relación con las acusaciones por hechos ilícitos que por su complejidad pudieran resultar más problemáticos y en los que precisamente se hace más necesaria esa unificación de criterios, entre ellos los relativos a delitos de acceso ilegal a sistemas, delitos de interceptación irregular de comunicaciones entre sistemas, delitos de daños informáticos, delitos relacionados con el abuso de dispositivos, delitos de pornografía infantil, en los que concurran subtipos agravados, delitos contra la propiedad intelectual y delitos competencia del área de especialización cuando sean cometidos por organización criminal, o se desarrollen o produzcan sus efectos en mas de una provincia. El efecto positivo que tiene, en orden a la unificación de criterios, esta labor de supervisión desde la Unidad Central, se vería incrementado si se ampliaran las atribuciones y competencias de muchos de los Delegados y secciones territoriales pues el más completo conocimiento y seguimiento de las causas por hechos ilícitos asignados al área de especialización haría posible un análisis mas detallado de los diversos problemas que están surgiendo en la investigación y enjuiciamiento de las conductas vinculadas al uso de las TIC.