11. CRIMINALIDAD INFORMÁTICA

11.1 **Introducción**

El uso de las Tecnologías de la Información y Comunicación (en adelante TIC,s) con finalidad delictiva es un fenómeno en permanente evolución tanto en los aspectos cualitativos como cuantitativos. En el primer sentido porque el propio desarrollo de las tecnologías determina una variación constante en las formas y/o medios de planificación y ejecución de las conductas susceptibles de lesionar bienes jurídicos necesitados de protección, y en el aspecto cuantitativo porque la generalización en el uso de estas tecnologías por los ciudadanos, y su puesta al servicio de todo tipo de actividades y de cualquier forma de relación personal, colectiva o institucional, hace que cada vez sea más frecuente la comisión de actividades ilícitas que o bien se llevan a efecto a través de esas tecnologías o bien tienen por objeto los propios datos y/ó sistemas informáticos.

Esta situación está determinando la necesidad de ofrecer respuestas ágiles y eficaces ante esta fenomenología criminal que incide de una u otra forma, pero en cualquier caso con efectos muy significativos, en muy diversas tipologías delictivas, dando lugar a la aparición de nuevas formas de lesión o puesta en peligro del bien jurídico afectado o a unas mejores condiciones de planificación y ejecución del *iter criminis* o de expansión y multiplicación de sus efectos. Tanto es así que una buena parte de la reforma del CP aprobada por LO 1/2015 de 30 de marzo alcanza a tipos penales vinculados a la criminalidad informática, como los delitos de pornografía infantil, de descubrimiento y revelación de secretos, de daños informáticos o los delitos contra la propiedad intelectual, y también a aquellos otros en los que la utilización de estas tecnologías está influyendo en las formas de ejecución de las conductas sancionables como ocurre con los crímenes de odio, los delitos contra la libertad o seguridad de las personas e incluso los delitos de terrorismo.

Pero la actuación frente a esta forma de delincuencia no solo exige de la modificación/adaptación de tipos penales o de la tipificación de nuevas conductas, sino que también es fundamental que el legislador provea a los investigadores y a los operadores jurídicos de herramientas aptas para esclarecer los hechos ilícitos que se cometen a través de estas tecnologías, lo que en definitiva significa regular el uso eficaz de los instrumentos y herramientas informáticas en la investigación criminal pero garantizando al tiempo el respeto al pleno ejercicio de los derechos y libertades de los ciudadanos. También en este ámbito el

legislador español está intentando ofrecer soluciones y con esa finalidad se ha elaborado un proyecto de ley para la reforma de aspectos parciales de la Ley de Enjuiciamiento Criminal, en el que se abordan muchos de los aspectos relacionados con la investigación tecnológica. Este proyecto iniciará próximamente su andadura parlamentaria, proceso en el que esperamos se introduzcan algunas mejoras en el texto inicial que estimamos necesarias.

En todo caso, no ha de olvidarse que la materia que nos ocupa no debe ser analizada aisladamente sino como la derivación, en el ámbito de la criminalidad, de un problema más amplio que es la necesidad de asegurar –en términos generales y en todos los ámbitos– la protección de los ciudadanos y de la actividad que la sociedad en su conjunto desarrolla en el ciberespacio. A ello responde la Estrategia de Ciberseguridad Nacional, publicada en diciembre de 2013, en la que se encuentran implicados todos los poderes públicos. A través de esta Estrategia se pretende por el *Gobierno implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas,* labor en la que el Ministerio Fiscal se encuentra directamente implicado como institución encargada constitucionalmente –también en el ciberespacio– de promover la acción de la Justicia en defensa de la legalidad, de los derechos de los ciudadanos y del interés público tutelado por la ley.

11.2 Análisis de diligencias de investigación y procedimientos judiciales incoados y acusaciones del Ministerio Fiscal en el año 2014

Los datos estadísticos obtenidos a partir de la información trasladada por las Fiscalías provinciales acerca de los hechos delictivos incluidos en la Instrucción 2/2011 de la Fiscalía General, *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías*, revelan que en el año 2014, llegaron a conocimiento del Ministerio Fiscal un total de 20.534 procedimientos judiciales por este tipo de ilícitos, lo que supone un incremento en un 71,21 % respecto de los 11.990 procedimientos registrados como tales en el año 2013 y en más de un 210 % respecto de los 6.532 identificados en 2011, año en el que inició su andadura esta área de especialización del Ministerio Fiscal.

Para garantizar una interpretación correcta de estos resultados ha de recordarse, como en anteriores Memorias, que uno de los problemas que complican el análisis de este fenómeno criminal es, precisa-

mente, la especial dificultad en la detección e identificación de los procedimientos judiciales/diligencias de investigación que tienen por objeto hechos ilícitos vinculados al uso de las TIC,s. Ello es consecuencia de la transversalidad de esta forma de delincuencia que puede manifestarse en comportamientos ilícitos de muy diversa naturaleza, y encuadrables en diferentes tipos penales, por lo que su reflejo a efectos estadísticos en muchas ocasiones puede quedar oculto en los datos globales correspondientes al registro genérico de los distintos delitos, circunstancia que ocurre siempre que no se deja constancia en las aplicaciones, con la debida precisión, del carácter informático de la infracción.

A resolver este problema ha dedicado este área de especialización una buena parte de su actividad durante los más de tres años de trabajo en la materia, y no solo por la importancia que tiene el control estadístico de estos procedimientos para conocer la incidencia y evolución en nuestro país de este fenómeno criminal sino también –y todavía más– porque únicamente de esta forma, conociendo las causas incoadas por estos ilícitos, estaremos en condiciones de hacer posible la intervención especializada del Ministerio Fiscal en todas ellas o, al menos, en las de mayor trascendencia y/o complejidad.

En anteriores Memorias ya hemos tenido la ocasión de explicar el sistema de trabajo establecido, en coordinación con las Fuerzas y Cuerpos de Seguridad, para adquirir un conocimiento temprano de todas estas investigaciones y para hacer posible su anotación registral y el control y seguimiento de las mismas, y a ello nos referiremos de forma más detallada en otros apartados de esta Memoria. Los datos que ofrecemos en esta ocasión son el producto de ese trabajo sostenido y sus resultados no pueden ser más evidentes ya que el número de procedimientos objeto de seguimiento por este área de especialización presenta unos índices al alza del 21,82 % entre los años 2011 y 2012; 50,64 % entre 2012 y 2013 y 71,21 % entre 2013 y 2014.

Ahora bien, este llamativo incremento a nuestro entender no puede interpretarse como una consecuencia derivada exclusivamente del aumento, en términos similares, en el numero de hechos ilícitos vinculados al uso de las TIC,s. Sin negar que ese sea el origen al menos de una parte de esos resultados, en ellos confluye también la evidente mejora en nuestra propia capacidad de detectar estas investigaciones y de anotarlas como tales en nuestras estadísticas y aplicaciones informáticas. La relativa estabilidad que se aprecia en los datos interanuales que proporcionan un numero destacable de Fiscalías provinciales nos lleva a pensar que el sistema establecido para la identificación de causas por ciberdelitos se encuentra ya consolidado en gran parte del

territorio nacional, por lo que en un futuro próximo estos resultados responderán de forma más fiel a la propia evolución de esta forma de delincuencia y su valor a efectos de analizar el fenómeno que nos ocupa será cada vez mayor. Ello sin perjuicio de reseñar que la cifra negra de criminalidad en este ámbito es incuestionablemente alta y especialmente en determinadas manifestaciones criminales, como los daños informáticos o los accesos ilegales a sistemas, en los que las denuncias –por desconocimiento, falta de confianza en el sistema o interés en proteger la propia reputación– son todavía llamativamente escasas.

11.2.1 Procedimientos incoados

El detalle de los datos sobre los procedimientos judiciales incoados en 2014, de acuerdo con nuestra información estadística es el siguiente:

	TOTAL	%
Daños, sabotaje informático	143	0,70
Acceso sin autorización	297	1,45
Descubrimiento y revelación de secretos	561	2,73
Contra los servicios de radiodifusión	15	0,07
Estafa	17.328	84,39
Acoso a menores de 13 años	60	0,29
Pornografía y corrupción de menores o discapacitados	581	2,83
Contra la propiedad intelectual	58	0,28
Falsificación documental	156	0,76
Injurias y calumnias contra funcionario público	381	1,86
Amenazas y coacciones	527	2,57
Contra la integridad moral	130	0,63
Apología o incitación a la discriminación	30	0,15
Otra tipología delictiva	150	0,73
– Denuncias por suplantación de identidad	117	0,57
TOTAL	**20.534**	**100,00**

Como fácilmente se constata, el volumen más alto de procedimientos corresponde a las denuncias por estafa, que sumaron un total de 17.328, lo que supone un porcentaje del 84 % del total de expedientes de esta naturaleza incoados en el año. Dicha proporción es similar a la detectada en años precedentes, si bien supera levemente el índice obtenido en el año 2013 que no alcanzó el 81 %. Es incuestionable por

tanto que los hechos asociados al uso de las TIC,s que los ciudadanos denuncian con más frecuencia, y en relación con los cuales se sienten más vulnerables, son los comportamientos ilícitos con finalidad defraudatoria.

No obstante también en este caso la interpretación correcta de estos datos exige de ciertas precisiones. La primera es, sin duda, que un volumen importante de estas denuncias tiene su origen en efectos o resultados individualizados de una misma acción criminal. Como es sabido la potencialidad expansiva de las herramientas tecnológicas determina frecuentemente que las consecuencias de la conducta criminal se generen en una pluralidad de territorios y puedan dar lugar por tanto a múltiples denuncias muchas de las cuales son catalogadas inicialmente como faltas –delitos leves del art. 249-2.º del nuevo texto del CP– al no superar el perjuicio causado a los perjudicados, individualizadamente considerados, la cantidad de 400 euros.

Esta circunstancia, que relativiza sin duda la importancia de las cifras que estamos comentando, implica no obstante una especial dificultad en la investigación de este tipo de actividades criminales ya que hace necesario que los Fiscales que integran esta área de especialización lleven a efecto una importante labor de coordinación, a veces con alcance trasnacional, que será objeto de comentario detallado en otro epígrafe de esta Memoria.

Por otra parte, también ha de aclararse que en el apartado que nos ocupa se incluyen una diversidad de comportamientos delictivos que, utilizando diferentes y novedosas dinámicas y aprovechando las ventajas que ofrecen las tecnologías, hacen posible la obtención ilícita de grandes beneficios a costa del perjuicio que originan en múltiples ciudadanos. Las manifestaciones más importantes de estas conductas, que genéricamente registramos como estafas, bien sea del párrafo 1.º bien del 2.º del art. 248 CP, son las ventas de productos u ofrecimiento de servicios de carácter fraudulento que se realizan a través de la red; las diversas técnicas defraudatorias de ingeniería social como el *phising*; la contratación fraudulenta de líneas telefónicas y los accesos inconsentidos a servicios de tarificación adicional; el conocido como *carding* y/o uso irregular de tarjetas de crédito o de sus datos o incluso de tarjetas virtuales y también determinadas actividades engañosas relacionadas con el juego on-line.

Cada una de estas modalidades de estafa presenta unas características distintas y una problemática diferente en su investigación y enjuiciamiento y, al igual que la generalidad de las actividades ilícitas que se cometen a través de la red, su mayor o menor incidencia y

sus formas de ejecución van variando y adaptándose a las nuevas situaciones derivadas del desarrollo tecnológico. Aun cuando todavía no estamos en condiciones de ofrecer datos individualizados de estas distintas modalidades defraudatorias, la información que manejamos a partir de las Memorias provinciales ya nos permite efectuar algunas consideraciones de interés, como la relativa al progresivo descenso en la utilización del modelo tradicional de estafa por *phising*, extremo que comentan diversas Fiscalías como las de Pontevedra, Granada o Guipúzcoa. Esta técnica utilizada generalmente por organizaciones criminales radicadas en otros países y consistente en ordenar fraudulentamente trasferencias bancarias –mediante la previa captación informática de las claves bancarias de sus víctimas y contratación en nuestro país de *mulas* encargadas, a cambio de una comisión, de recepcionar los fondos sustraídos y remitirlos a los responsables últimos de la acción criminal– está siendo abandonada para ser sustituida por otros modelos de estafa. La razón de este cambio de tendencia puede estar en la implementación de nuevas medidas de seguridad por las entidades bancarias, como es el caso de los sistemas de autenticación de doble factor o las contraseñas de uso único, pero también puede haber contribuido a ello el importante volumen de acusaciones presentadas en los últimos años contra las personas que han actuado como *mulas*, circunstancia que ha servido para dar publicidad a la naturaleza delictiva de este tipo de operaciones, dificultando la posibilidad de alegar un supuesto desconocimiento del carácter ilícito de los fondos, argumento esencial de defensa de los imputados por estas conductas

Por su parte, los procedimientos incoados por delitos contra la libertad e indemnidad sexual de los menores cometidos a través de las TIC,s ascendieron el pasado año a 641, un 3,12 % del total de los registrados en el marco de la criminalidad informática. En este apartado incluimos tanto los relativos a delitos de pornografía infantil y/o de personas con discapacidad que sumaron 581 como los derivados de denuncias de acoso a menores a través de estas tecnologías previstos en el art. 183 bis CP, que ascendieron a 60.

En relación con los primeros, se detecta un ligero incremento, en un 11 %, respecto del año 2013, en el que se iniciaron 521 procedimientos por estos tipos delictivos. Sin embargo ese resultado alcista se relativiza si tenemos en cuenta que porcentualmente en 2014 estos expedientes supusieron tan solo un 2,82 % del total de los incoados por hechos ilícitos vinculados a las TIC,s, en tanto que este índice en el año 2013 fue del 4,35 %. En cualquier caso la cifra resulta significativamente baja y, pese a ese pequeño repunte, da cuenta de una tendencia claramente descendente que se viene observando desde el inicio de la actividad de esta área, ya que los 818 procedimientos registrados en 2011 que implicaron un 12,52 % del total, descendieron a 619 en 2012, representando un índice porcentual del 7,78 %.

Como ya indicamos en Memorias precedentes, sería erróneo interpretar estos datos como el resultado de una disminución del volumen o frecuencia con que se cometen estas concretas actividades ilícitas. Más bien al contrario, la generalización en el uso de las TIC,s ha potenciado extraordinariamente este tipo de conductas y ha determinado una mayor facilidad para el acceso de cualquier ciudadano a material pornográfico. Son bastantes las Memorias provinciales en las que se informa acerca de esa tendencia descendente y se analizan las razones de ello. Es precisamente esa experiencia la que nos permite afirmar que la reducción en el volumen de procedimientos hay que buscarla en la modificación de los medios o sistemas a través de los cuales se consume o distribuye dicho material, circunstancia que ha generado mayores dificultades en la detección e investigación de estos comportamientos por parte de los cuerpos policiales. Así, el tradicional intercambio de archivos a través de las redes P2P –fácilmente rastreables por los cuerpos policiales– se ha ido abandonando en favor de la utilización, para la obtención ó difusión de contenidos ilícitos, de redes y foros privados de acceso restringido, en los que la posibilidad de penetración de los investigadores es muy limitada o incluso a través de otros medios de comunicación como Whatsapp o Skype ó de sistemas de intercambio difícilmente detectables, como el almacenamiento del material pornográfico en archivos en la nube compartidos por dos o más personas.

No obstante estas dificultades, el empeño de investigadores y operadores jurídicos y el aprovechamiento y utilización de las propias herramientas informáticas en la investigación criminal determinan que se sigan obteniendo resultados eficaces frente a este tipo de conductas generando incluso el leve incremento en el volumen de procedimientos a que anteriormente nos hemos referido. Ese es el objetivo

con el que se está trabajando y a ello contribuirán, sin duda, algunas de las medidas que contempla el proyecto de reforma parcial de la Ley de Enjuiciamiento Criminal, recientemente aprobado por el Gobierno, como las mejoras introducidas en la figura del agente encubierto, al igual que el reforzamiento de la cooperación internacional en esta materia y el intercambio de información con organismos internacionales como Europol, Eurojust ó el National Center for Prevention of Missing and explotation Children (Agencia Gubernamental americana de lucha contra la pederastia). Al respecto es interesante reseñar la participación de la Fiscalía española, representada por la Fiscal Delegada de Madrid, en un equipo conjunto de investigación constituido con autoridades judiciales de Suecia y República Checa para actuar de forma coordinada ante una operación internacional de elaboración y distribución de pornografía infantil.

La persecución de estos tipos penales se verá también potenciada por la reciente reforma del Código Penal. Como acertadamente se reseña en la Exposición de Motivos de la LO 1/2015, la sanción, en el párrafo 2.º del nuevo artículo 189-5, del *streaming* y/o acceso *on-line,* a sabiendas, a contenidos de esta naturaleza, va a hacer posible la persecución de conductas que hasta el momento resultaban atípicas. A su vez, la previsión especifica en el Código Penal de la retirada o bloqueo, por decisión judicial, de páginas web que contengan material ilícito contribuirá, sin duda, a minimizar los efectos de estas criminales acciones.

Los procedimientos incoados por delitos de acoso a menores de 13 años a través de las TIC,s sumaron 60 en el año 2014, lo que supone un leve descenso, de un 13 %, respecto a las 69 causas de este tipo que se registraron en 2013. Se trata de un precepto que, por las propias exigencias del tipo penal, ha sido escasamente aplicado desde su incorporación al Código Penal por LO 5/2010 de 22 de junio, habiendo sido reconducidos muchos comportamientos de esta naturaleza a otros tipos penales, cuando las víctimas eran mayores de trece años o cuando no se cumplía algún otro de los requisitos del tipo. La reciente reforma de esta figura delictiva como consecuencia de la elevación a 16 años de la edad para prestar consentimiento sexual y la extensión de la conducta típica que se contempla en el párrafo segundo del nuevo artículo 183 ter afectará en el futuro a las posibilidades de aplicación de este precepto.

Significativo sin duda es el aumento de los procedimientos por delitos de descubrimiento y revelación de secretos que ascienden a 858, un 4,17 % del total de los incluidos en ámbito de competencia de la especialidad, de los que 297 corresponden a investigacio-

nes por delitos de acceso ilegal a sistemas cuya sanción ha estado prevista, hasta la reciente reforma, en el art. 197-3.º CP. Estos resultados evidencian un repunte de casi el 60 % en el conjunto de las tipologías delictivas sancionadas en el artículo 197 CP y del 52,30 % en cuanto a las conductas de acceso ilegal a sistemas, en referencia en ambos casos a los resultados obtenidos por esos mismos conceptos en el año 2013. Se mantiene por tanto la tendencia alcista que se venía observando en años precedentes y que en el caso del acceso ilegal a sistemas se concreta en un incremento del 156 % entre los años 2012 y 2013 y de un 70 % de 2011 a 2012. En muchos casos se trata de supuestos de utilización no autorizada de cuentas de correo ajenas o de acceso irregular a perfiles de redes sociales para suplantar, con diversas finalidades, la identidad de los verdaderos titulares.

También se incrementan notablemente, en un 70 %, los expedientes sobre daños informáticos que ascienden a 143 frente a los 84 registrados en 2013, pese a lo cual la cifra sigue siendo llamativamente baja a tenor de la información sobre *ciberataques* que facilitan los organismos e instituciones de carácter público o privado expertos en esta materia. La tendencia al alza se mantiene año a año a partir los 62 procedimientos de este tipo incoados en 2011 –primera anualidad en que se efectuó un control específico de los mismos– pero sigue siendo necesario fomentar la presentación de denuncias e impulsar las investigaciones de estas acciones ilícitas. Posiblemente la publicación de la Estrategia de Ciberseguridad Nacional contribuya a ese objetivo ya que en la misma se aboga por articular instrumentos que canalicen el traslado de información sobre incidentes de seguridad con connotaciones delictivas a los órganos encargados de la investigación y persecución penal.

Los delitos contra la propiedad intelectual dieron lugar en el año memorial a 58 nuevos procedimientos judiciales, un 80 % más que en 2013. En ello, sin duda, ha influido la publicación, el 8 de abril del pasado año de la Sentencia dictada por el TJUE en el asunto Svensson, cuya interpretación abierta del concepto de comunicación pública –una de las conductas típicas que recoge el artículo 270 CP– permite catalogar como tal la actividad consistente en facilitar enlaces para el acceso irregular a obras protegidas, siempre que concurran el resto de los requisitos que exige el tipo penal. De hecho en las Conclusiones de las Jornadas de Especialistas celebradas en mayo de 2014, aprobadas posteriormente por la Fiscalía General del Estado, se acordó asumir esta interpretación del concepto de comunicación pública para

amparar la persecución penal de estas conductas y ese mismo es el espíritu que subyace en la reforma operada en esos tipos penales por LO 1/2015 de 30 de junio.

Al igual que el pasado año estimamos oportuno englobar en un único apartado una diversidad de comportamientos que inciden en la intimidad, la libertad, la integridad moral o el honor de las personas, y en ocasiones también en el prestigio de las instituciones, y que cada vez con mayor frecuencia se planifican y ejecutan a través de estas tecnologías de la información y la comunicación. En el año 2014 hemos constatado como en ocasiones determinadas y por razones de índole muy diversa se han producido una pluralidad de comentarios ofensivos, humillantes o insultantes vertidos de forma indiscriminada en las redes sociales o en Twitter que han puesto en riesgo bienes jurídicos de carácter individual o colectivo. Circunstancias tan diversas o aleatorias como el asesinato de un responsable político, o la derrota de un equipo deportivo nacional frente al conjunto que representaba al Estado de Israel, dieron lugar a una oleada de comentarios en foros y redes sociales cuya trascendencia penal fue preciso analizar jurídicamente a través de la incoación de una pluralidad de diligencias de investigación penal y/o procedimientos judiciales.

Pero además, también estamos detectando, y a ello se refieren expresamente muchas Memorias provinciales, la utilización creciente de estas herramientas contra personas perfectamente determinadas a las que a través de estos medios se pretende humillar, acosar, amenazar, ofender o incluso desprestigiar públicamente causándoles un grave daño moral. Llaman la atención los Delegados sobre el uso frecuente de estas vías de comunicación en el ámbito de la violencia contra la mujer y también, y muy especialmente, en las relaciones entre personas menores de edad, dado que los agresores pueden utilizarlas de forma ágil, sencilla y eficaz para lograr su ilícitos propósitos y amplificar, al tiempo, los efectos perniciosos sobre sus víctimas.

La actuación frente a esta clase de conductas presenta unas dificultades especiales dado que, a las propias de toda investigación criminal, se suman las derivadas del carácter técnico del medio empleado que, en ocasiones y si se utilizan por expertos, puede complicar extraordinariamente la determinación del responsable criminal de la infracción. Además la adecuada tipificación de estos comportamientos exige de un estudio individualizado de cada uno de los contenidos o, en su caso, de todos los contenidos atribuidos a una misma persona. No es infrecuente que en una misma comunicación o en un único comentario efectuado a través de la red se incorporen expresiones intimidatorias o amenazantes junto a otras de carácter injurioso o

degradante. En consecuencia la calificación jurídica de estos comportamientos puede hacerse, según las circunstancias, como delito de amenazas, de coacciones, de injurias –perseguibles de oficio en los supuestos del art. 215 CP– e incluso como delitos contra la integridad moral del art. 173.1 del mismo texto legal.

El análisis de la evolución de los datos estadísticos sobre procedimientos por delitos de esta naturaleza, que abordamos conjuntamente por las razones indicadas, revela que en el año 2014 estas conductas dieron lugar a un total de 1.038 expedientes judiciales, poco más de un 5 % del total de procedimientos incoados por hechos ilícitos vinculados al uso de las TIC,s.

El volumen más elevado corresponde sin duda a los delitos de amenazas y coacciones con 527 registros, cuyo porcentaje de crecimiento, superior a un 111 %, respecto al año 2013, da buena cuenta de la progresiva incidencia del uso de las tecnologías en la ejecución de estas ilícitas acciones. Los 381 registros correspondientes a delitos de injurias y calumnias a funcionario público, muestran un notable incremento, en este caso del 64 % respecto del año precedente. Por su parte, los procedimientos incoados como delitos contra la integridad moral descienden levemente, en un 18 %, respecto de mismo dato obtenido en el año anterior.

Finalmente, y en cierta medida vinculados a estos comportamientos, no podemos dejar de referirnos a los llamados crímenes de odio y a los de justificación del genocidio en los que también se está percibiendo claramente el impacto de la utilización de las TIC,s. En el año 2014 registramos 30 procedimientos por esta clase de ilícitos, lo que supone un incremento del 114 % respecto de los 14 registros efectuados en 2013 y la recuperación de las cifras obtenidas en 2012 en que se incoaron 28 expedientes por esas tipologías delictivas. Al respecto es de interés reseñar que varios de los procedimientos judiciales incluidos en este grupo derivan de las Diligencias de Investigación n.º 2/2014 y 3/2014 de la Unidad Central del área de especialidad incoadas por denuncias presentadas por colectivos de la comunidad judía en relación con diversos contenidos de carácter antisemita difundidos a través de internet tras el acontecimiento deportivo al que anteriormente se ha hecho referencia.

No podemos acabar este análisis sin referirnos, siquiera someramente, a las cifras que computamos en el apartado «otras tipologías delictivas». Se incluyen en ese epígrafe los procedimientos incoados como consecuencia de denuncias por acciones cometidas a través de las TIC,s y no encuadrables en ninguno de los tipos penales específicamente reseñados, como, por ejemplo, los supuestos finalmente cali-

ficados como blanqueo de capitales en las defraudaciones por phising; determinadas conductas asociadas a la violencia de género cometidas a través de las TIC,s, ó incluso denuncias presentadas por comentarios de carácter ofensivo realizados a través de la red y considerados *ab initio* atípicos. Pero sin duda el volumen más elevado –y de ahí su mención independiente– son los procedimientos derivados de denuncias por suplantación de identidad en la red que han dado lugar, al menos, a 117 incoaciones en el año 2014. El hecho de que no se haya tipificado expresamente en nuestra legislación esta conducta determina que estos comportamientos, salvo que puedan reconducirse a otros tipos penales como el descubrimiento y revelación de secretos o los delitos contra la integridad moral entre otros, no den lugar a responsabilidad penal y el procedimiento se vea abocado al archivo.

11.2.2 Escritos de acusación del Ministerio Fiscal

El análisis que abordamos a continuación ofrece sin duda un una información mucho más detallada y completa de la actividad del Ministerio Fiscal en esta materia y también de la eficacia de la respuesta del Estado de Derecho ante esta forma de delincuencia. No olvidemos que, a diferencia de lo que ocurre en la fase de incoación del procedimiento judicial, en la que los contornos de la actividad ilícita no se encuentran todavía suficientemente definidos, la presentación del escrito de acusación por parte de la Fiscalía implica que se ha culminado la fase de investigación procesal, se ha esclarecido suficientemente el hecho denunciado y se han hallado pruebas suficientes para imputar su comisión a persona o personas concretas y determinadas. Por tanto las conclusiones que se pueden obtener en este apartado se basan en información muy fiable y debidamente depurada a lo largo de la tramitación procesal.

Según los datos facilitados por las Fiscalías provinciales el numero de acusaciones por hechos ilícitos encuadrables en el ámbito de la criminalidad informática de acuerdo con los parámetros establecidos en la Instrucción 2/2011 de la Fiscalía General del Estado ascienden a un total de 1275, lo que refleja un leve ascenso, en un 1,03 %, respecto de las 1.262 calificaciones presentadas en el año 2013. El volumen de escritos de acusación presentados en procedimientos por hechos ilícitos vinculados a este área de especialidad ha ido ascendiendo año a año –906 en 2011; 1092 en 2012; 1262 en 2013 y 1275 en el año memorial– si bien el ritmo de progresión se ha ido ralentizando hasta

concretarse en este último periodo en 13 escritos de acusación en cifras absolutas. El detalle por tipologías delictivas es el siguiente:

ACUSACIONES	TOTAL	%
Daños, sabotaje informático	11	0,86
Acceso sin autorización	40	3,14
Descubrimiento y revelación de secretos	76	5,96
Contra los servicios de radiodifusión	11	0,86
Estafa	577	45,25
Acoso a menores de 13 años	10	0,78
Pornografía y corrupción de menores o discapacitados	285	22,35
Contra la propiedad intelectual	24	1,88
Falsificación documental	29	2,27
Injurias y calumnias contra funcionario público	17	1,33
Amenazas y coacciones	93	7,29
Contra la integridad moral	17	1,33
Justificación genocidio/incitación discriminación	4	0,31
Otra tipología delictiva	81	6,35
TOTAL	**1.275**	**100,00**

Al igual que en los años 2012 y 2013 el volumen más elevado de acusaciones corresponde a delitos de estafa, con un total de 577 escritos, un 45,25 % del total general. Sin embargo resulta llamativo que por primera vez se quiebra la tendencia alcista pues la cifra revela un descenso en las acusaciones de poco más de un 6 % en referencia a los 618 escritos de acusación por estos tipos delictivos formulados en el año 2013. La proporción entre el volumen de procesos iniciados y acusaciones formuladas por estos ilícitos, poco más del 3,3 %, es llamativamente baja y tiene su explicación en la dispersión territorial de los efectos de la acción ilícita, a los que antes nos hemos referido y en la circunstancia de que, en muchas ocasiones, los responsables criminales actúan desde otros países lo que dificulta extraordinariamente su identificación y enjuiciamiento.

Siguen en importancia, por su volumen, las acusaciones formuladas por delitos de pornografía infantil, 285 que suponen el 22,35 % del conjunto de las formuladas en 2014. También en este caso se detecta un descenso, de un 6,5 %, respecto de las 305 calificaciones que se presentaron por esta clase de infracciones en el año 2013. Al igual que en otras anualidades y por contraste con otras figuras delictivas, como es el caso de la estafa, es destacable el elevado número de procedimientos sobre estos ilícitos que finalmente dan lugar a la presentación

de escrito de acusación. Con las reservas, derivadas del hecho de que un número no precisado de las acusaciones presentadas en 2014 lo fueron en expedientes incoados en años anteriores, el resultado de la comparación de ambos datos ofrece un índice del 49 %, extraordinariamente revelador de la eficacia de los investigadores y de los órganos de la jurisdicción penal en esta materia que se ve favorecido por la circunstancia de que en estos asuntos la investigación se centra en acciones de fabricación, distribución y/o posesión realizadas íntegramente en nuestro país y constatables a partir del análisis de los dispositivos informáticos incautados al responsable criminal.

Precisamente por ello resulta obligado llamar la atención, una vez más, sobre el inconveniente que supone para la tramitación de estas causas el retraso en la elaboración de informes periciales, extremo sobre el que alertan muchos de los Delegados y que debería ser abordado a través de una más completa dotación de los gabinetes científicos de los cuerpos policiales, tanto en medios personales como materiales, y también mediante el establecimiento de pautas uniformes que hagan posible limitar el recurso a ese tipo de informes exclusivamente a aquellos supuestos en los que dicho dictamen resulte necesario ó justificado.

Consideración independiente merecen las acusaciones presentadas por delitos de amenazas que se elevan en 2014 a un total de 93, con un notable incremento cifrado en un 69 % en relación con los escritos elaborados por igual concepto en 2013 y de un 244 % en relación con la cifra obtenida en 2012. También ofrecen una tendencia al alza los escritos de acusación sobre delitos contra la integridad moral que, con una cifra de 17, recogen un incremento del 140 % respecto del ejercicio anterior. Estos datos avalan sin duda las reflexiones anteriormente efectuadas acerca de la incidencia creciente del uso del TIC,s en la ejecución de conductas ilícitas que atentan contra bienes de carácter personal. La comparación, con las salvedades antes indicadas, entre procedimientos incoados y los escritos de acusación presentados es del 17,64 % en el primer caso y del 13,07 % en los delitos contra la integridad moral.

Se aprecia igualmente el incremento en el numero de acusaciones relativas a delitos de descubrimiento y revelación de secretos, que sumaron el año memorial un total de 116, poco más de un 9 % del total de las presentadas en 2014, reflejo de un ligerísimo ascenso en un 5 % respecto de los formulados por estos delitos en el año 2013. El volumen más importante de ellos, concretamente 76 de dichos escritos, tuvieron por objeto delitos de acceso ilegal a sistemas del artículo 197-3 del CP.

Acusan también un notable crecimiento los datos sobre escritos de acusación presentados por delitos contra la propiedad intelectual que suman 24, recuperándose valores ligeramente superiores al año 2012 tras el notable descenso acusado en 2013, anualidad en la que solo se formularon 14 escritos de acusación en esta categoría. Este resultado es acorde al detectado en referencia a los procedimientos iniciados por estos mismos ilícitos y puede ser debido, al menos en parte, a la interpretación abierta del concepto comunicación pública propiciada por la sentencia de 8-IV-2014 del Tribunal de Justicia de la Unión Europea, a la que antes nos hemos referido.

11.2.3 Diligencias de Investigación

Las Diligencias de Investigación incoadas por el Ministerio Fiscal el pasado año, al amparo del artículo 5 del nuestro Estatuto Orgánico y del artículo 773 de la LECrim, ascendieron a un total de 65, incrementándose por tanto en más de un 22 % el resultado obtenido por igual concepto en el año 2013. Como ya hemos tenido ocasión de señalar en anteriores Memorias, la reducida cifra de este tipo de expedientes tiene su razón de ser en que las investigaciones sobre hechos ilícitos cometidos a través de las TIC,s, por afectar a derechos fundamentales, como intimidad o secreto de las comunicaciones, requieren generalmente de autorización judicial para la práctica de muchas de las diligencias imprescindibles para el esclarecimiento del hecho y la determinación de sus autores, lo que aboca necesariamente a su judicialización ante el órgano competente para ello.

DILIGENCIAS DE INVESTIGACIÓN	TOTAL	%
Daños, sabotaje informático	1	1,54
Acceso sin autorización	2	3,08
Descubrimiento y revelación de secretos	5	7,69
Estafa	10	15,38
Acoso a menores de 13 años	2	3,08
Contra la propiedad intelectual	2	3,08
Injurias y calumnias contra funcionario público	12	18,46
Amenazas y coacciones	4	6,15
Justificación genocidio/incitación, discriminación	23	35,38
Otro tipo delictivo	4	6,15
TOTAL	**65**	**100,00**

El desglose por tipos penales de las Diligencias de Investigación incoadas evidencia que el volumen más elevado de ellas, 23 en cifras absolutas que suponen más de un 35 % del total de las correspondientes al año memorial, lo fueron por delitos de justificación del genocidio o incitación al odio o a la discriminación, seguidas por las 12 iniciadas por supuestos delitos de injurias y calumnias a funcionario público.

En uno y otro caso, estas actuaciones están motivadas por las denuncias recibidas directamente en la Fiscalía con ocasión de los comentarios ofensivos o humillantes vertidos a través de twitter o de las redes sociales, en momentos puntuales del año memorial y que, como hemos comentado, se centraron en determinados colectivos definidos por su religión, ideología política u otras circunstancias. Precisamente dos de estas Diligencias de Investigación fueron incoadas en la propia Unidad Central y tuvieron por objeto una pluralidad de comentarios atribuidos a una diversidad de usuarios, lo que necesariamente dio lugar a un análisis separado e individualizado de cada uno de ellos, que se concretó finalmente, en algunos de esos supuestos, en la presentación de denuncias ante los órganos judiciales competentes.

En atención a los resultados obtenidos también merecen ser reseñadas, las 10 diligencias de investigación incoadas por delitos de estafa, las 5 que lo fueron por delitos de descubrimiento y revelación de secretos y las 4 que tuvieron por objeto denuncias sobre amenazas o coacciones a particulares.

11.3 Organización interna del Área de Especialidad. Relación con otros servicios de la Fiscalía

Las reflexiones realizadas hasta el momento dan buena cuenta de la evolución del fenómeno criminal que nos ocupa y de cómo el uso creciente de las TIC,s con finalidad criminal está demandando cada vez una mayor atención de los investigadores y de los órganos de la Administración de Justicia.

La percepción de estas circunstancias, y la experiencia adquirida después de tres años de trabajo específicamente orientado a la actuación ante esta forma de criminalidad, ha determinado la consolidación de los servicios territoriales de la especialidad, la delimitación –cada vez más clara– de las atribuciones encomendadas a los Delegados en cada una de las Fiscalías provinciales y, en definitiva, el reforzamiento de la actividad que corresponde desempeñar a este área de especiali-

zación, como contribución al cumplimiento de la misión atribuida constitucionalmente al Ministerio Fiscal en el marco de la jurisdicción penal.

Conscientes de esta realidad, en la reunión de Delegados, celebrada con ocasión de las Jornadas de Especialistas en el mes de mayo del pasado año, se adoptaron determinadas conclusiones orientadas a mejorar la planificación y los resultados de nuestro trabajo y también a garantizar una actuación cada vez más coherente y eficaz de la Institución en este ámbito. Concretamente se fijaron tres grandes líneas de acción: a) hacer posible una más completa detección e identificación y, en consecuencia, control e intervención en las diligencias de investigación/procedimientos judiciales por hechos ilícitos vinculados al uso de las TIC,s; b) extender el ámbito de acción de la especialidad a la totalidad del territorio provincial estableciendo los mecanismos de colaboración necesarios con las Fiscalías de Área y Secciones Territoriales; c) potenciar una actuación coherente y uniforme del Ministerio Fiscal en esta materia promoviendo y facilitando una mayor colaboración con aquellos servicios especializados en materias en las que la incidencia del uso criminal de las TIC,s es más evidente.

En cuanto al primer aspecto, como ya hemos tenido ocasión de mencionar, el carácter transversal de esta forma de criminalidad y la circunstancia de que se manifieste a través de muy diversas tipologías delictivas, ha supuesto desde el inicio una seria dificultad para la identificación –lo más temprana posible– de los expedientes relativos a estos ilícitos como requisito imprescindible para hacer posible la intervención en su tramitación de quienes integran este área de especialización. En ello se viene invirtiendo un gran esfuerzo, a nivel territorial y nacional, no solo por parte de los Fiscales sino también y muy especialmente de las Fuerzas y Cuerpos de Seguridad, nacionales y autonómicas que, con encomiable disponibilidad, están colaborando estrechamente con la Fiscalía para informarnos puntualmente de cuantos atestados se tramitan por hechos de esta naturaleza con el objetivo de facilitar nuestra labor de detección y seguimiento de los mismos.

El resultado de este trabajo está claramente a la vista. El incremento en un 71,21 % en el volumen de causas sobre este tipo de delitos de los que ha tenido conocimiento el Ministerio Fiscal en el último año, da cuenta de que la dinámica seguida al respecto es la adecuada. Como resultado de ello cada año disponemos de una mejor información acerca la evolución de estas tipologías delictivas y estamos en condiciones de asegurar la intervención especializada del Ministerio

Fiscal en la instrucción y enjuiciamiento de estos ilícitos o al menos de aquellos que son más graves o presentan una mayor complejidad.

A su vez la constatación de la creciente incidencia del fenómeno que nos ocupa esta determinando un efecto derivado, ya comentado en la anterior Memoria y ahora claramente perceptible: el reforzamiento de los servicios territoriales y la ampliación progresiva del número de Fiscales que integran el área de especialización. Efectivamente la percepción en los órganos territoriales de la Institución de la evolución de esta forma de delincuencia y de la complejidad técnica que en muchas ocasiones implica su investigación y enjuiciamiento, ha generado que muchos de los Fiscales Jefes, a partir de la valoración de estas circunstancias en el respectivo ámbito de competencia, hayan estimado conveniente ampliar los efectivos personales al servicio de la sección de criminalidad informática, de tal modo que en la actualidad casi la mitad de las Fiscalías españolas cuentan con más de un Fiscal encargado específicamente de esta materia.

Ha de recordarse que cuando iniciamos el trabajo de la red de especialistas en el año 2011, contábamos para ello únicamente con un Fiscal Delegado en cada una de las 50 Fiscalías provinciales así como con el imprescindible apoyo, en la Unidad Central, de la Ilma. Sra. doña Ana María Martín Martín de la Escalera en calidad de Fiscal adscrita. Al momento de elaborar esta Memoria el numero de Fiscales asignados a esta materia superan levemente la centena y al menos 13 de las delegaciones territoriales cuentan con personal administrativo adscrito para facilitar las tareas encomendadas a la sección, datos expresivos por si mismos del crecimiento experimentado aunque es cierto, y así ha de aclararse, que en muchos territorios –como en las Fiscalías provinciales de Madrid o Las Palmas– la misma sección se ocupa conjuntamente del área de Criminalidad Informática y de la de Tutela Penal de la Igualdad y contra la Discriminación. En cuanto a la Unidad Central, integrada únicamente por dos personas, se ha visto ampliada a partir del mes de marzo de 2015 con la incorporación de una nueva Fiscal adscrita la Ilma. Sra. doña Pilar Rodríguez que hasta ahora venía ejerciendo de forma encomiable la función de Fiscal delegada de la especialidad en la sección territorial Madrid.

La ampliación de efectivos dedicados a la especialidad está permitiendo también ampliar el catalogo de atribuciones que desempeñan las secciones en cada una de las Fiscalías. Sin perjuicio de recordar que las circunstancias específicas de cada provincia –en lo que a volumen de asuntos y disponibilidades de la plantilla orgánica se refiere– determinan necesariamente criterios diferentes en la distribución del trabajo, es un hecho constatado que las secciones de esta especialidad

poco a poco van extendiendo las funciones encomendadas en los distintos territorios.

En algunos casos como las Fiscalías provinciales de Bizcaia, Castellón, Guipúzcoa, Palencia, Las Palmas, Santander, Soria o Valladolid, el servicio asume la intervención en la totalidad de los procesos por hechos de esta naturaleza y en muchos de los juicios orales derivados de los mismos. En otros casos los especialistas solo se encargan plenamente de una parte de los asuntos sobre ilícitos vinculados al uso de las TIC,s, definidos bien sea por criterios estrictamente territoriales o por la asignación especifica de determinadas materias por decisión del Fiscal Jefe. Ejemplo significativo del primer supuesto es la Fiscalía de Madrid, cuya sección especializada asume la intervención en todos los asuntos sobre ciberdelitos de la Fiscalía provincial, encargándose del visado de los correspondientes a las Fiscalías de Área, o también la sección de criminalidad informática de Cádiz, cuyo delegado, integrado en la Fiscalía de Área de Jerez de la Frontera, se encarga de todos los expedientes de la especialidad en el ámbito territorial de este último órgano.

La asignación de asuntos por razón de la materia obedece también a criterios diferentes en atención a las peculiaridades de cada Fiscalía. Los procedimientos por delitos de pornografía infantil son los que con más frecuencia se encuentran encomendados específicamente a los servicios de criminalidad informática, en ocasiones conjuntamente con los correspondientes a otras tipologías delictivas como el acoso a menores a través de las TIC,s (Fiscalía de Málaga), los delitos contra la propiedad intelectual (Fiscalía de Valencia), los delitos de daños informáticos, descubrimiento y revelación de secretos y estafas (Fiscalía de A Coruña), los delitos comprendidos en el apartado III de la Instrucción 2/2011 FGE (Fiscalía de Ciudad Real) o en términos generales cualquier delito que presente especial complejidad (Fiscalías de Cáceres y Pontevedra). Finalmente en un número destacable de órganos provinciales la asignación de asuntos a la sección se lleva a efecto esencialmente en atención a la gravedad del hecho o la especial dificultad de la investigación con independencia de cuál sea la tipología delictiva investigada (Fiscalías de Barcelona, Girona o Navarra).

Pero en todo caso, haya o no asignación concreta de asuntos, el Delegado provincial por sí mismo o apoyado por quienes integran la sección se encarga del control e impulso de los procedimientos que nos competen así como de colaborar con los compañeros, y promover una actuación coherente y eficaz del Ministerio Fiscal en esta materia, de acuerdo con criterios uniformes. Esta labor se facilita a través del visado de escritos de acusación y de sobreseimiento, función que se

ha encomendado al propio Delegado en algunas Fiscalías como A Coruña, Cádiz, Castellón, Granada, Illes Balears, León, Málaga, Madrid, Santander, Sevilla, y Valencia. Esta misma circunstancia también se produce por razones obvias, en aquellos otros órganos en los que el propio Fiscal Jefe asume esta delegación, concretamente en Albacete, Guadalajara, Cuenca, Burgos, Valladolid, Zamora y Orense. En otros territorios, como Almería, Gerona, Lérida, Huelva, Segovia y Toledo, el Delegado colabora con el Fiscal Jefe en el ejercicio de esta atribución, a través una revisión previa –previsado– del escrito de acusación o informe sometido a la consideración de aquél.

Ya hemos dicho que un aspecto esencial en la organización de los servicios territoriales es el de identificación y seguimiento de los procedimientos por hechos de esta naturaleza, actuación especialmente compleja por la pluralidad y diversidad de manifestaciones típicas y por el incremento en el volumen de procedimientos. Por ello resulta incuestionable la importancia de prestar una especial atención al registro informático de causas, a la anotación de la naturaleza de la infracción en las distintas fases de los procesos y/o al control de carpetillas. A esos efectos se valora muy positivamente la opción adoptada en al menos 13 Fiscalías provinciales de dotar a las secciones de criminalidad informática de un apoyo administrativo específico para facilitar la gestión y el control informático de los expedientes por delito vinculados al uso de las TIC,s, de ahí, nuestro interés en promover la aplicación de ese mismo sistema en todas Fiscalías sin que ello tenga por que implicar una dedicación exclusiva a esta actividad sino solo una atención centralizada de la Secretaría al registro informático y al seguimiento de la evolución procesal estos procedimientos.

La segunda línea de acción antes referida pretende que los efectos de la especialización alcancen a la totalidad del respectivo territorio provincial, con independencia del órgano del Ministerio Fiscal en que tenga su sede la Delegación correspondiente. Ha de recordarse que salvo en los escasos supuestos en que la sede del servicio radica en una Fiscalía de Área –Jerez de la Frontera (Cádiz); Vigo (Pontevedra) y Alcoy (Alicante)– su localización se encuentra en la Fiscalía provincial, generalmente en la capital a excepción del de la Fiscalía de Teruel que se ubica en la sección territorial de Alcañiz. Es obvio –y así se entendió en las últimas Jornadas de Especialistas– que el diferente despliegue territorial del Ministerio Fiscal en los distintos ámbitos provinciales en ningún caso debe afectar a las competencias de los servicios especializados que abarcan toda la extensión de la demarcación provincial. Por ello, para hacer efectivo ese planteamiento, y facilitar la coordinación y el traslado de información, muchos de los

servicios territoriales de criminalidad informática se han ido articulando mediante el establecimiento de puntos de enlace/contacto con aquellos otros órganos del Ministerio Fiscal constituidos en la misma provincia y en los que no radica la sede física de la Delegación.

Así, el servicio territorial de Cádiz, ubicado en la Fiscalía de Área de Jerez de la Frontera cuenta con puntos de enlace en las Fiscalías de Área de Algeciras y Ceuta; el de Las Palmas, con sede en la capital, integra especialistas pertenecientes a las Fiscalías de Área de Arrecife-Puerto del Rosario y San Bartolomé de Tirajana y tiene enlaces en dos de los partidos judiciales de la isla de Gran Canaria; el de Barcelona cuya sede radica en la Fiscalía provincial se completa con puntos de enlace en las Fiscalías de Área de Granollers y Mataró-Arenys de Mar y en la Sección Territorial de Badalona; el de Badajoz cuenta con un punto de enlace en la Fiscalía de Área de Mérida y el de Pontevedra, con sede en la Fiscalía de Área de Vigo, integra a un Fiscal especialista en la Fiscalía provincial; el de Illes Balears, centralizado en la capital mallorquina, tiene establecidos enlaces en la Fiscalía de Área de Ibiza y en las Secciones Territoriales de Mahón y Manacor. Con todo, el servicio que, por el momento, ofrece una articulación más completa es sin duda el de Madrid que, con sede en la capital y atendido por tres personas junto con el Delegado, cuenta además con puntos de enlace permanentes en las Fiscalías de Área de Alcalá de Henares; Getafe-Leganés y Móstoles y en las Secciones Territoriales de Collado Villalba; Majadahonda-Pozuelo y Alcobendas.

Al margen de los supuestos antes indicados, en los que el objetivo es facilitar la coordinación con otros órganos territoriales del Ministerio Fiscal, son otras muchas las Fiscalías en las que labor del Delegado se completa con el apoyo, en el propio órgano, de algún otro miembro del Ministerio Fiscal. Tal es el caso de las Fiscalías de A Coruña, Albacete, Ciudad Real, Guipúzcoa, Málaga ó Sevilla, si bien es especialmente significativo el caso de la Fiscalía de Valencia cuyo servicio de criminalidad informática lo integran siete Fiscales además del Delegado. En muchos de estos casos, la composición plural del servicio ha servido para facilitar la relación con las sedes de la propia Fiscalía provincial que se encuentran distanciadas geográficamente de la capital. Buen ejemplo de ello es el servicio de la Fiscalía Tarragona, con puntos de enlace en las Secciones Territoriales de Tortosa y Reus y en el partido judicial de El Vendrell; el de Girona, que integra un Fiscal en el partido judicial de Figueres; el de Almería con enlace en El Ejido; el de Tenerife en el que se integra un Fiscal de la Sección Territorial de Arona; el de Bizcaía, que integrada por tres miembros en la sede capitalina tiene un punto de contacto permanente en la Sección

Territorial de Baracaldo; el de Asturias cuyo delegado provincial es apoyado por un coordinador designado a dicho fin tanto en la Sección Territorial de Avilés como en la de Langreo o el de Castellón que a sus cuatro miembros en la sede provincial suma un enlace en la Sección Territorial de Vinaroz.

Todo este despliegue, que se ha llevado a efecto en los poco más de tres años de funcionamiento de esta área de especialización, da buena cuenta del esfuerzo y la ilusión con la que la Institución en su conjunto se está volcando en actuar de una forma eficaz frente a estas nuevas manifestaciones criminales, haciendo posible en cualquier punto de la geografía nacional una intervención permanente y dinámica del Ministerio Fiscal en los procedimientos por delitos de esta naturaleza, una más intensa colaboración con los organismos e instituciones con responsabilidad en esta materia, incluidas las Fuerzas y Cuerpos de Seguridad y una mayor y más eficiente aproximación al ciudadano que favorezca la presentación de denuncias por quienes son víctimas de estas acciones criminales, así como la subsiguiente investigación y persecución de las mismas.

Como tercera línea de acción, se acordó en las últimas Jornadas de Especialistas, ahondar en la unificación de criterios y en la acción coherente y uniforme en todas aquellas áreas de actividad del Ministerio Fiscal que tienen por objeto materias en las que está teniendo incidencia el uso criminal de las TIC,s. Como ya hemos mencionado las características de esta forma de delincuencia hace que sus efectos se extiendan a manifestaciones criminales que competen a otras áreas de especialización. Esta circunstancia determina que, en una Institución regida por los principios de unidad de actuación y dependencia jerárquica, constituya una prioridad trabajar coordinadamente y aprovechando la experiencia y conocimientos de los distintos servicios especializados para ofrecer soluciones conjuntas a los problemas que plantea la investigación y enjuiciamiento de estos comportamientos delictivos.

Desde un punto de vista subjetivo el sector de la población que más profundamente se está viendo afectado por el desarrollo de las TIC,s es sin duda el de los jóvenes y adolescentes, que son los que con más frecuencia y en mas alto porcentaje hacen uso de estas tecnologías para cualquier tipo de actividad. Como consecuencia de ello los integrantes de este colectivo son también víctimas preferentes de muchos de los delitos cometidos a través de las TIC,s, y no solo de las conductas que atacan su libertad o indemnidad sexual sino también de otro tipo de actividades ilícitas como las amenazas, el acoso o los atentados contra la intimidad personal. También, en no pocas ocasio-

nes, este uso generalizado de las TICs determina que personas menores de edad aparezcan como responsables de acciones delictivas cometidas a través de estas herramientas.

Por ello uno de los objetivos que nos hemos propuesto –a nivel nacional y en los distintos territorios– es estrechar la colaboración con el área de especialización en la atención y tratamiento a menores de edad. Son muchas las memorias de las Fiscalías provinciales en las que se insiste en este tema y son diversas las soluciones que se han ido articulando para facilitar el necesario trabajo conjunto en la resolución de cuantas cuestiones de interés común se planteen. Así en algunas Fiscalías, como las de León e Illes Balears, el Delegado de Criminalidad Informática lo es también del área de Menores, y en otras como las de Huesca y Badajoz se encuentra integrado en las secciones territoriales de dicha especialidad. En otras provincias, como Pontevedra, Valencia y Guipúzcoa, han optado por incluir dentro del servicio de criminalidad informática a algún Fiscal perteneciente a la sección de menores o que trabaje directamente vinculado a ella, o incluso al propio Delegado de dicha sección, como es el caso de Castellón. En los restantes supuestos las Fiscalías refieren una colaboración fluida y permanente tanto en lo que se refiere al intercambio de experiencias y conocimientos como incluso al traslado de información sobre actuaciones realizadas y expedientes en curso.

En una u otra forma es patente el esfuerzo que se está realizando en los distintos territorios para facilitar esta actuación coordinada entre ambas áreas, conscientes como somos de que esta preocupante forma de criminalidad no solamente incide en la actuación en vía de reforma respecto de personas menores de edad sino también en los aspectos relacionados con la protección de sus derechos como víctimas frecuentes y especialmente vulnerables de estas actividades ilícitas.

Llaman también la atención los Fiscales sobre el incremento de los supuestos en que delitos relacionados con violencia contra la mujer aparecen vinculados al uso de las TICs. Amenazas, coacciones, delitos contra la intimidad o contra la integridad moral se están cometiendo, cada vez con más frecuencia, a través de estas tecnologías, lo que en muchas ocasiones implica una complejidad añadida en la investigación o enjuiciamiento de los mismos. Por ello en muchos territorios se está reforzando la colaboración entre ambas áreas de especialidad con las mismas finalidades antes indicadas. También en este caso, en algunas Fiscalías se ha tomado en consideración esta circunstancia para la organización del servicio de criminalidad informática, tal es el caso de la Fiscalía de Castellón que integra en

el mismo al Delegado provincial de la Sección de Violencia contra la Mujer.

Ya nos referimos en la Memoria del pasado año a la intensa vinculación de esta materia con el área de Tutela Penal de la Igualdad y contra la Discriminación, dada la progresiva utilización de las redes sociales e internet para difundir el discurso del odio o incluso para plantear y organizar actos concretos de violencia por motivos discriminatorios derivados de la raza, la nacionalidad, la ideología, la orientación sexual, la situación de discapacidad… etc. Tanto es así que durante el año 2014 ambas áreas de especialización han estado coordinadas, a nivel nacional, por un mismo Fiscal de Sala. Esta circunstancia y el hecho de que en más de la mitad de las Fiscalías provinciales ambas materias fueran responsabilidad de un mismo Delegado o de idéntico servicio, ha contribuido extraordinariamente a facilitar la unificación de criterios y el planteamiento de actuaciones conjuntas ante comportamientos que afectaban a ambas especialidades.

En lo que concierne a este último objetivo, hemos de mencionar también la conveniencia, sugerida por diversos Fiscales, de establecer mecanismos para estrechar la colaboración con quienes integran la red de Fiscales de cooperación internacional. El carácter trasnacional de los ciberdelitos determina que con frecuencia sea necesario recurrir a solicitudes de auxilio judicial internacional activas o pasivas y, sin duda, en la tramitación de las mismas es de gran ayuda la colaboración con los fiscales especializados en ello. Resulta necesario no obstante, y a ello se refieren algunos Fiscales, mejorar el traslado de información entre ambas áreas acerca de las comisiones rogatorias que se cursan por hechos de esta naturaleza para facilitar la coordinación de actuaciones en relación con estos comportamientos que, en no pocas ocasiones, se desarrollan en sus distintas fases o producen sus perniciosos efectos en diferentes países.

Coordinación de investigaciones

Para concluir este apartado debemos referirnos a otro de los objetivos prioritarios que se marcó este área de especialización desde sus inicios enfocado a facilitar la coordinación de investigaciones derivadas de un mismo ilícito o de ilícitos conexos cuando sus manifestaciones se presentan en una pluralidad de territorios. Nos enfrentamos a una forma de delincuencia que, por su propia naturaleza y características, frecuentemente se desarrolla y/o produce efectos en distintas

provincias lo que da lugar a la apertura de tantas investigaciones como lugares se vean afectados, bien porque en ellos se ha materializado alguna de las fases de ejecución de la actividad delictiva, bien porque constituyen el lugar de residencia de los perjudicados por la misma. La importancia de la coordinación de estas investigaciones no solo reside en la necesidad de evitar las indeseadas dilaciones provocadas por reciprocas inhibiciones entre los órganos judiciales concernidos, con el consiguiente riesgo de pérdida o inutilización de las evidencias electrónicas, sino que también resulta esencial para que la respuesta penal que se proporcione al delito sea global y adecuada a su verdadera entidad.

Como señalan algunos Delegados la coordinación de las investigaciones que tienen por objeto hechos de esta naturaleza se convierte en un elemento esencial para garantizar su resultado y en esta labor contamos con la ventaja de que nuestra propia organización interna nos permite articular coherentemente la adecuada respuesta a éste fenómeno. Es por ello que la primera de las conclusiones alcanzadas en las Jornadas de Especialistas, celebradas en el mes de mayo del pasado año, se refiere a *la importancia de la labor de la red de Fiscales de criminalidad informática para hacer posible, en esta área de actividad, la necesaria coordinación de las investigaciones incoadas con ocasión de los múltiples efectos que una misma actividad ilícita puede generar en distintos puntos del territorio nacional* y –tras subrayar el valor que tiene a esos efectos la capacidad de coordinación interna y de actuación conforme a criterios uniformes del Ministerio Fiscal– insta a los Fiscales Delegados para que, en cumplimiento de lo dispuesto en la Instrucción 2/2011 de la Fiscalía General del Estado, extremen su atención para comunicar a la Unidad Central cuantas investigaciones lleguen a su conocimiento por actividades ilícitas que trasciendan fuera de su ámbito territorial de competencia con el fin de que en ésta última se inicien las labores de coordinación que procedan en relación con ello.

Es de significar que esta labor se ha visto favorecida por la constitución, a partir del mes de febrero del año 2014, de sendas oficinas de enlace con el Cuerpo Nacional de Policía y la Guardia Civil, ambas ubicadas en las propias dependencias de la Unidad Central en la calle José Ortega y Gasset, a las que se da traslado de las solicitudes de coordinación para informar sobre cuantas diligencias policiales hayan sido incoadas en sus respectivos cuerpos por hechos*, a priori,* relacionados con aquellos cuya acumulación se pretende.

El trabajo que, en éste concreto aspecto, realizan los funcionarios responsables de ambas oficinas de enlace, con la posibilidad de

acceso directo a sus correspondientes bases de datos policiales, sin duda ha facilitado la obtención de información relacionada con las investigaciones que han de ser coordinadas. Pero también ha contribuido a mejorar esta labor la consolidación y refuerzo de las secciones especializadas, a la que ya se ha hecho referencia en otro apartado de esta Memoria, pues, gracias al sistema permanente y fluido de comunicación interna existente entre los Fiscales especialistas que integran la Red tanto a nivel central como en cada una de las Fiscalías territoriales, las decisiones se han adoptado desde un conocimiento más amplio tanto del contenido de las diligencias en curso en los distintos lugares de la geografía nacional, como de su alcance y estado de desarrollo, potenciando de esta forma nuestra capacidad para fijar criterios uniformes y promover, cuando así se ha estimado oportuno la acumulación de procedimientos, evitando intervenciones dispersas, descoordinadas o incluso contradictorias entre sí que, en definitiva, proporcionan a los autores una mayor facilidad en la ejecución del delito cuando no garantizan su propia impunidad.

En el año 2014 casi todos los expedientes de coordinación impulsados desde la Unidad Central se han incoado a solicitud de los Fiscales delegados cuando, en el ejercicio de su actividad, verificaban que los hechos objeto de investigación habían dado lugar a otras denuncias presentadas por perjudicados de distintos puntos de territorio nacional. En su mayoría se ha tratado de actuaciones de coordinación referidas a actos defraudatorios –estafas con múltiples perjudicados– que se han llevado a efecto mediante la publicación de anuncios engañosos en distintas páginas web tales como Ebay.es, milanuncios.com, segundamano.com…, etc., ofreciendo en venta productos inexistentes con el solo objeto de lograr la transferencia de dinero por parte de las personas interesadas en su adquisición que, una vez pagaban, nunca recibían el objeto comprado.

Para la coordinación resulta necesario identificar, en la medida de lo posible, todas las diligencias de investigación y/o procedimientos incoados por hechos vinculados entre sí en cualquier punto de la geografía nacional que conformen la acción ilícita. A tal fin se recaban los pertinentes informes tanto de las unidades de enlace con la Fiscalía como de las policías autonómicas –si bien en éste caso a través de los Fiscales delegados del territorio correspondiente –y se completa la información remitida con la que obtienen los propios Fiscales especialistas mediante consulta de sus respectivas bases de datos.

Todas las diligencias identificadas en dichos informes son objeto de análisis en la Unidad Central con el fin de determinar cuáles deben ser objeto de acumulación por referirse a una misma actividad delic-

tiva, ejecutada por una misma persona o varias de común acuerdo, y descartar aquellas en las que no concurra tal circunstancia o que simplemente no pueden ser acumuladas por tratarse de cosa juzgada, haber prescrito o encontrarse en una fase procesal que no permita tal posibilidad.

Una vez se aprecia la necesidad de acumulación resulta necesario determinar el fuero territorial competente para conocer de las diligencias acumuladas. En relación con ello ha de recordarse que estas investigaciones por delitos informáticos con perjudicados en diversos territorios genera, conforme al criterio de la ubicuidad avalado por el Pleno no jurisdiccional del TS de fecha 3 de febrero de 2005, una pluralidad de fueros comisivos. Según esta doctrina, el delito se entiende cometido en todas las jurisdicciones en los que se haya realizado algún elemento del tipo: bien sea el lugar o lugares en los que ha desarrollado la acción/es el sujeto activo, bien donde el sujeto pasivo lleva a cabo el desplazamiento patrimonial, bien donde se produce el perjuicio patrimonial.

Ante esta pluralidad de fueros comisivos, resulta necesario determinar qué juzgado resulta competente para la tramitación conjunta de todas las acciones conexas. La Fiscalía en éste punto concreto se ha acogido a la más reciente doctrina del Tribunal Supremo promoviendo que la acumulación de las diligencias se efectúe ante el órgano judicial competente del territorio donde se encuentran las pruebas del delito. En éste sentido, los ATS de 17/5/12, 9/10/14, 23/10/14 y 14/11/14, al resolver cuestiones de competencia planteadas por delitos de estafa informática con pluralidad de perjudicados, han sostenido como criterio más idóneo el del lugar donde se descubren las pruebas del delito porque, aun cuando el criterio de la ubicuidad parece priorizar el lugar de domicilio de los perjudicados y apuntar la competencia del juzgado que primero incoó procedimiento por denuncia de cualquiera de ellos, rara vez será éste el territorio donde se encuentren las evidencias del ilícito pues habitualmente su responsable ha llevado a cabo la acción mediante conexiones a internet realizadas desde su propia residencia, y es éste también el lugar donde normalmente domicilia las cuentas bancarias para ingreso de sumas defraudadas y en donde usualmente dispone de las mimas.

Con todo, los avances conseguidos por éste área de especialización en la coordinación de investigaciones conexas siguen siendo insuficientes pues se trata de una labor que continua planteando muchos problemas aún pendientes de resolver. Hoy por hoy resulta prácticamente imposible tener la absoluta certeza de que se han examinado la totalidad de las diligencias derivadas de una misma activi-

dad ilícita sea cual sea el punto del territorio nacional donde sean conocidas. La falta de unas bases de datos comunes a todos los cuerpos policiales, nacionales y autonómicos, que hagan saltar las alarmas tan pronto como por la dinámica comisiva del hecho o su presunta autoría se evidencia la posible conexión con otras diligencias ya incoadas, unida a la existencia de distintos sistemas informáticos judiciales, según el territorio autonómico de que se trate, imposibilita no solo el conocimiento completo de todos los asuntos relacionados entre sí, sino también que el trabajo de coordinación se lleve a cabo ágilmente por cuanto, la obtención de la información necesaria –a través de los distintos cuerpos policiales y de la propia Fiscalía –se demora en el tiempo y su análisis tardío determina que en muchas ocasiones resulte imposible ó poco operativa la acumulación que se pretende.

Desde la Unidad Central, a solicitud de las Fuerzas y Cuerpos de Seguridad, también se han llevado a cabo las necesarias gestiones para garantizar la actuación coordinada de los Fiscales delegados en diversas operaciones policiales que han requerido intervenciones simultáneas en distintas demarcaciones territoriales. En tal sentido es de reseñar, como destacan algunos de Delegados, que el conocimiento anticipado de estas diligencias ha redundado en el éxito de muchas de estas operaciones de entre las que cabe destacar en el año 2014 las denominadas operación Dustman, de la Guardia Civil contra la pornografía infantil, y la operación Doscar de la Policía Nacional seguida por delitos contra la propiedad intelectual.

Por último reseñar la coordinación desde la Unidad Central de la participación del área de especialización en equipos conjuntos constituidos en Eurojust para facilitar investigaciones transnacionales en las que España se encontraba involucrada. La intervención a nivel central se ha efectuado cuando la investigación en España aun se encontraba en fase policial desconociéndose por tanto el Juzgado a que iba a corresponder su conocimiento.

A destacar en este sentido la participación de la Fiscalía en llamada «operación Eurimus» desarrollada con el objetivo de desmantelar una organización delictiva que se valía de programas o malwares creados al efecto, para llevar a cabo intrusiones en los sistemas informáticos de distintas empresas de las que se descargaban bases de datos con información sobre tarjetas de crédito y usuario de sus clientes que después vendían a terceros para su ilícito uso y también en la denominada «operación Onymous» dirigida contra mercados clandestinos de Internet en la que, tras geolocalizarse en Arenys de Mar (Barcelona) una página Web desde la que supuestamente se estaba llevando a efecto la venta de euros falsos a cambio de bitcoins, la participación

del Fiscal Delegado de Barcelona, designado a tal efecto por la Fiscal de Sala, resultó decisiva para poder materializar la práctica simultánea con Europa y Estados Unidos de las diligencias de entrada y registro acordadas. En esta última operación la actuación de la Fiscalía española ha sido objeto de felicitación desde Eurojust.

11.4 Relaciones con Instituciones u Organismos Públicos o Privados y con las Fuerzas y Cuerpos de Seguridad

Según refieren los Delegados ya se encuentran plenamente consolidadas las vías de relación establecidas en años anteriores con Fuerzas y Cuerpos de Seguridad y con otros organismos e instituciones. En general se desatacan las fluidas relaciones con los cuerpos policiales y su colaboración en la identificación de los procedimientos mediante la adopción de las medidas necesarias para ello.

En la misma línea desde la Unidad Central se ha dado continuidad a los vínculos de colaboración ya establecidos con los organismos e instituciones, tanto del sector público como del privado involucrados en la erradicación de la ciberdelincuencia, que ya fueron objeto de comentario detallado en la Memoria de 2013. La frecuente participación de la Unidad Central en reuniones y grupos de trabajo en los que se han tratado aspectos técnico jurídicos relacionados con la investigación y tipificación de los delitos informáticos (así con los Ministerios de Justicia y Educación, Cultura y Deporte, Incibe, Foro de colaboración Público-Privada en Ciberseguridad, Colegios de Abogados… etc.) ha dotado a la Fiscalía de mayor visibilidad y ello ha determinado un incremento en el número de denuncias remitidas directamente por estos organismos a la Fiscalía especializada para su valoración y tratamiento.

Por su parte, la puesta en marcha de las Unidades de enlace, a la que ya nos hemos referido, ha supuesto que a nivel central se hayan intensificado las relaciones de colaboración con ambos cuerpos policiales. Son usuales las sesiones de trabajo para analizar investigaciones concretas y los específicos problemas de carácter jurídico legal que pueden plantear, así como para establecer las líneas de actuación que contribuyan al éxito de las mismas.

En el marco de las relaciones institucionales mantenidas por la Unidad Central debemos hacer mención a la comparecencia ante la Subcomisión de Estudio de Redes Sociales del Congreso de los Diputados, llevada a cabo por la Fiscal de Sala Coordinadora en representación de la Fiscalía General del Estado, el 22 de abril de 2014. El

objetivo de la misma –al igual que el de la comparecencia efectuada en el Senado en el año 2013– fue trasladar al poder legislativo la visión del Ministerio Fiscal sobre la problemática que plantea la investigación de las conductas ilícitas que se cometen a través de la red así como efectuar sugerencias de reforma legislativa en relación con ello. Las conclusiones de la Comisión constituida en el Senado, recogidas junto con las aportaciones de los comparecientes en el Informe publicado en el Boletín Oficial de las Cortes el 3 de octubre del año memorial, se han reflejado en algunos de los aspectos que se abordan en el proyecto de reforma procesal, como es el caso de la previsión de hacer extensiva la técnica policial del agente encubierto a la investigación de cualquier de delito cometido a través de las TICs con independencia de la gravedad o naturaleza del mismo.

Consideración aparte merece también la intervención de la Unidad Central del área de especialización, a través de la Fiscal de Sala y por designación expresa del Ministerio de Justicia, en las dos reuniones del TC-Y de la Convención de Budapest del Consejo de Europa, celebradas respectivamente los días 16 y 17 de junio y 2 y 3 de diciembre del pasado año. En ambos casos y como es habitual las conclusiones obtenidas en el transcurso de dichos encuentros fueron trasladas al Ministerio de Justicia a los efectos de la adecuada implementación de las directrices de dicha Convención en nuestra normativa interna. También aquí la labor realizada se ha visto reflejada en la previsión en el proyecto de reforma de la Ley de Enjuiciamiento Criminal de la orden de conservación de datos, como medida de aseguramiento de evidencias electrónicas de interés en posteriores investigaciones penales a través de la cual se incorpora en nuestra norma procesal el artículo 16 del mencionado Convenio.

Finalmente es obligado referirse a la intervención del Ministerio Fiscal en el desarrollo de la Estrategia de Ciberseguridad Nacional. Como ya indicamos al inicio de esta Memoria, dicha Estrategia que se aprobó en diciembre de 2013, es el documento que sirve de fundamento al Gobierno de España para desarrollar las previsiones en materia de protección del cibersespacio, objetivo que, a su vez, se desglosa en seis de carácter más específico, uno de los cuales, a los efectos que aquí interesan, se centra *en potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación ante las actividades de terrorismo y la delincuencia en el ciberespacio.*

Para el desarrollo de esta Estrategia y de sus líneas de actuación, se constituyeron el pasado año 2014 varios grupos de trabajo en los que se integran representantes de los diversos departamentos ministe-

riales con responsabilidad en esta materia. El Ministerio de Justicia propuso la intervención del Fiscal de Sala de Criminalidad Informática en representación de la Fiscalía General del Estado en dos de estos grupos: el referente a la línea de actuación cuarta relativa a la lucha contra la ciberdelincuencia y el ciberterrorismo y el destinado al desarrollo de la línea de acción sexta dedicada al compromiso y la cooperación internacional en esta materia.

El primero de estos grupos está trabajando específicamente en tres ámbitos: el planteamiento de propuestas de reforma legislativa en atención a las necesidades detectadas para hacer frente a esta forma de criminalidad, la mejora de capacidades frente al ciberterrorismo y la ciberdelincuencia a través de una mayor colaboración de los encargados de la investigación y la persecución penal con los organismos con responsabilidad en materia de ciberseguridad y también en los aspectos relacionados con la formación de operadores jurídicos y en particular del Ministerio Fiscal pues no en vano uno de los ejes de esa línea de acción es precisamente el *de asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado*. A dicho fin se sugiere en la Estrategia la necesaria cooperación, entre diversos organismos entre ellos la Fiscalía General del Estado o el Consejo General del Poder Judicial.

Por su parte en el segundo de los grupos indicados lo que se pretende es impulsar una mayor intervención e implicación de España en los foros e iniciativas internacionales sobre esta materia mediante actuaciones de carácter general y otras de naturaleza mas especifica como las de potenciar la red 24/7 de la Convención de Budapest o la red de Fiscales expertos en cibercrimen que se está articulando desde Eurojust o la de impulsar una mayor participación en los cursos o seminarios de carácter internacional para formación e intercambio de experiencias entre operadores jurídicos y/o investigadores de diversos Estados.

Con esta participación del Ministerio Fiscal en los grupos de trabajo para el desarrollo de la estrategia de Ciberseguridad Nacional, pretendemos contribuir a través de la aportación de nuestra experiencia y conocimientos, a mejorar la seguridad y la protección de los derechos de los ciudadanos en el ciberespacio.