COMPARECENCIA DE LA FISCAL DE SALA COORDINADORA CONTRA LA CRIMINALIDAD INFORMÁTICA, DÑA. ELVIRA TEJADA DE LA FUENTE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES CELEBRADA EL DÍA 27 DE JUNIO DE 2013.

La señora **FISCAL DE SALA COORDINADORA CONTRA LA CRIMINALIDAD INFORMÁTICA (**Dª Elvira Tejada de la Fuente): Muchísimas gracias señoría. En primer término, en nombre del Ministerio Fiscal español, en el de mi compañera doña Consuelo Madrigal Martínez-Pereda, como Fiscal de Sala Coordinadora en materia de Menores, y en el mío propio, quiero agradecer la oportunidad que nos dan de comparecer en esta interesantísima ponencia.

Primeramente quisiera recordar, como sus señorías saben, que el Ministerio Fiscal español es una institución de relevancia constitucional, que tiene unas funciones asignadas por la propia Constitución entre las cuales están la defensa de la legalidad, de los derechos de todos los ciudadanos y del interés público tutelado por la ley. El Ministerio Fiscal se rige por cuatro principios fundamentales, que también recoge el artículo 124 de la Constitución, que son los de legalidad, imparcialidad, unidad de actuación y dependencia jerárquica.

Y creo que es importante hacer referencia a los dos últimos porque, aunque son principios en torno a los cuales se articula, digamos, la

estructuración y organización interna de la Fiscalía, tienen una proyección externa muy importante ya que, gracias a la vigencia de esos principios, el Ministerio Fiscal actúa de acuerdo con una unidad de criterio y ello contribuye a garantizar la seguridad jurídica y la igualdad de todos los ciudadanos ante la ley, que son valores que también proclama nuestra Constitución.

Los Fiscales tenemos encomendadas muchas funciones, numerosas atribuciones que concreta nuestro Estatuto Orgánico y que comprenden no solamente la actuación que asumimos en el ámbito jurisdiccional penal sino también en otros ámbitos jurisdiccionales. Así, entre otras, desempeñamos funciones muy importantes de carácter tuitivo en relación con los más desvalidos, con los discapaces y con los menores de edad. Para poder desarrollar adecuadamente todas estas funciones nos hemos ido estructurando, sobre todo en estos últimos años, en áreas de especialización. Precisamente por ello, teniendo en cuenta que el objeto de esta ponencia es analizar la problemática que entraña la ciberdelincuencia, concretada especialmente en los riesgos que genera en los menores de edad, la comparecencia del Ministerio Fiscal en este acto se lleva a efecto a través de las personas que coordinamos las dos áreas de especialidad que confluyen en este tema: por una parte el área de criminalidad informática y, por otra, el área que se ocupa de protección y responsabilidad de los menores de edad.

Después de esta pequeña presentación, y entrando de lleno en la materia propia de mi competencia que es el área de criminalidad informática, me van a permitir que para centrar el tema haga primero unas valoraciones de carácter general: estamos ante un fenómeno criminal que no se circunscribe a delitos concretos, es decir, a un catálogo previamente determinado de delitos, sino que el concepto, en realidad, hace referencia a un fenómeno criminal que afecta a bienes jurídicos muy diversos y que

puede servir de soporte a conductas delictivas muy variadas. De hecho más que ante un grupo de delitos estamos ante una forma de cometer ilícitos de muy distinta naturaleza que, no obstante, presentan todos ellos una serie de características comunes que, para dar una visión de carácter general, podrían resumirse fundamentalmente en tres apartados.

Primero la complejidad técnica que ofrecen estas investigaciones y el enjuiciamiento de estas conductas, lo cual genera unas dificultades significativas para los que carecemos de una formación especifica en la estructura y funcionamiento de las tecnologías, digamos, para los que tenemos una preparación eminentemente jurídica. En relación con estas actividades ilícitas resulta más complicado descubrir el delito, encontrar las pruebas ó determinar quiénes son los delincuentes, porque en muchas ocasiones ello exige el conocimiento de unas técnicas, instrumentos o herramientas en cuyo manejo, en principio, no somos expertos. Por contra ¿qué nos encontramos?, frente a nosotros tenemos a unas personas que suelen ser unos expertos manejando estas tecnologías y que saben utilizarlas para multiplicar las consecuencias de la actividad criminal y, lo que es más importante a efectos de persecución penal, para ocultarse y dificultar su identificación. Internet ofrece múltiples mecanismos para anonimizar las conductas y ello supone un primer problema para actuar ante esta forma de delincuencia.

La Fiscalía, está dando respuesta a esta situación basándose en dos parámetros que son fundamentales y que están muy relacionados entre sí: formación y especialización (luego me referiré un poquito más en detalle a este último aspecto).

Segundo tema, segunda característica común a estas actividades ilícitas, la especial vulnerabilidad en la que se encuentra cualquier ciudadano, y en especial los que son más débiles, los que están más desprotegidos, como los menores, ante esta forma de delincuencia. ¿Por

qué? Porque se ha generalizado el uso de estas tecnologías entre todos los ciudadanos; porque ha penetrado en todas las facetas de nuestra vida, en nuestras relaciones a nivel personal, a nivel profesional, a nivel de ocio; porque sin querer, consciente o inconscientemente, estamos continuamente volcando en la red información sobre nosotros mismos que nos identifica perfectamente y que facilita que nos convirtamos en blanco de actividades ilícitas que pueden cometerse por personas que no conocemos, y con las que posiblemente jamás hubiéramos llegado a tener contacto fuera de la red: o sea, a veces, con nuestra propia actuación, nos colocamos un poco en el "punto de mira" de los ciberdelincuentes. Esto es especialmente llamativo, grave y peligroso en referencia a los menores de edad.

¿Qué ocurre además? Que el delincuente tiene a su favor un instrumento de fácil manejo que le permite potenciar los efectos de la actividad ilícita. Centrándonos en el tema de los menores de edad piensen, por ejemplo, que el daño que se le puede realizar a un niño con un trato degradante ó humillante a través de las redes es mucho más grave que el que se le puede originar en un contexto del mundo real porque a través de las redes sociales la ofensa se expande en cuestión de minutos a todo el haz de relaciones de la víctima y, en consecuencia, el perjuicio puede ser mucho más grave.

Y finalmente la tercera característica, que estimo muy importante y de especial relevancia en esta sede, es la necesidad de los ordenamientos jurídicos, de absolutamente todos los Estados, de mantener un proceso de adaptación permanente para ir dando respuesta a las situaciones nuevas que se van generando. Nos hallamos ante una realidad cambiante, ante una realidad que evoluciona muy, muy deprisa al hilo del desarrollo tecnológico, y que continuamente nos enfrenta a situaciones nuevas no previstas por la norma jurídica. Refiriéndome concretamente al ámbito que me corresponde, en mi responsabilidad como Fiscal encargada de

criminalidad informática, incidiría en dos grandes campos: el del derecho penal sustantivo y el de la investigación y el derecho procesal.

En el marco penal sustantivo es fundamental ir generando tipos penales que den respuesta a las nuevas conductas que se están produciendo, o ir adaptando los tipos ya existentes a la comisión de las correspondientes conductas a través de las tecnologías de la información y la comunicación, con el objetivo de disponer de una norma que haga posible la persecución y sanción de estos comportamientos capaces de lesionar bienes jurídicos merecedores de protección. Hay en curso ahora mismo un importante proyecto de reforma del Código Penal, al que luego me referiré específicamente, que aborda justamente la regulación de algunos tipos penales relacionados con el uso de las TIC´s y que nos interesan especialmente por afectar a menores de edad.

Y por otra parte el aspecto procesal, el aspecto de investigación, es también esencial. Porque estamos ante una forma de delincuencia en la que no sirven en términos generales como mecanismos de investigación muchas de las técnicas policiales de carácter más tradicional. Quiero decir con ello que, para investigar un delito cometido a través de la red, de poco van a servir, en muchos casos, técnicas como, por ejemplo, los seguimientos o las vigilancias policiales sino que este tipo de investigaciones exigirá, generalmente, utilizar en la indagación los propios sistemas informáticos. Y el problema es que en la actualidad no disponemos en nuestro ordenamiento jurídico de una regulación específica sobre muchos de los instrumentos legales que serían necesarios para ello.

Además esta cuestión es de especial importancia si tenemos en cuenta que tanto los ordenadores como los sistemas informáticos son herramientas –vamos a llamarlos así– capaces de almacenar una gran cantidad de información de carácter personal, y aptos para canalizar todas nuestra comunicaciones con terceros y a dicho fin están siendo utilizados

de forma generalizada. En consecuencia muchas de las investigaciones que tienen por objeto estas herramientas pueden incidir de forma clara y evidente en derechos fundamentales de la persona y especialmente en los derechos a la intimidad personal y al secreto de las comunicaciones, amparados en el artículo 18 CE. Como ustedes bien saben cualquier investigación que afecte a derechos fundamentales exige unas garantías, unos cuidados muy especiales en la adopción de las medidas, en la realización de la investigación, para no lesionar los citados derechos. Es por ello que resulta fundamental que cuanto antes se aborde una regulación adecuada de nuevas técnicas de investigación que permitan una actuación más eficaz frente a esta forma de delincuencia, garantizando, al tiempo, los derechos de los ciudadanos y la integridad y autenticidad de las evidencias que se vayan obteniendo.

No obstante he de aclarar que no estamos trabajando en vacío. Existen preceptos en la vigente Ley de Enjuiciamiento Criminal que pueden ser aplicados, y de hecho están siendo aplicados, en estos supuestos y disponemos de una Jurisprudencia y una doctrina del Tribunal Constitucional muy constante, muy consolidada y muy clara acerca de los parámetros que deben observarse en cualquier actividad de investigación que incida en derechos fundamentales. Y todo ello está sirviendo de base y fundamento en las actuaciones en curso. Pero sería bueno, como he indicado, que a la mayor brevedad posible se establecieran legalmente mecanismos específicos que ya están siendo necesarios para llevar adelante estas investigaciones con eficacia y con total seguridad y garantía.

Ante esta situación, el Ministerio Fiscal español se ha encontrado ante el reto por una parte de dar respuesta a estas situaciones y conseguir ser cada vez más eficaces ante esta forma de criminalidad y, por otra parte, de no ceder ni un ápice en nuestra función de defender los derechos y las libertades fundamentales. En esta circunstancia nuestra apuesta ha sido

por la especialización: articular un área de especialización en esta materia que, sobre la base de una formación permanente y continua, permita mejorar y potenciar nuestras habilidades y destrezas en este ámbito.

Ello ha dado lugar a la constitución de una red de Fiscales, especialistas en la materia, que tengo el honor de dirigir en estos momentos y que se despliega por todo el territorio nacional. En la actualidad contamos con una unidad central, radicada en esta capital, y un servicio de criminalidad informática, en todas las fiscalías provinciales, que se integra por el delegado de la especialidad auxiliado de uno o más compañeros en atención a la actividad de la respectiva fiscalía (volumen de procedimientos, plantilla orgánica, dimensión territorial provincial etc.). A partir de esta estructura trabajamos en equipo, a través de una comunicación interna fluida y constante, poniendo en común nuestras experiencias y nuestras opiniones que, valoradas conjuntamente, nos permiten ir elaborando esos criterios comunes que son los que posteriormente, una vez refrendados por la Fiscalía General del Estado, aplicamos en el desarrollo de nuestra actividad y en nuestra actuación ante los órganos judiciales.

Este trabajo en equipo, bajo los principios de legalidad y de imparcialidad, hace de esta área de especialización la *punta de lanza* del Ministerio Fiscal en la lucha contra este fenómeno criminal, porque esa experiencia compartida, y la preparación y conocimientos de los que nos vamos dotando, aprovechan a los restantes Fiscales, a la Institución en su conjunto, de tal modo, que nuestra labor es la de ir abriendo camino, ofreciendo soluciones ante este complejo fenómeno con tres objetivos fundamentales: potenciar las investigaciones por hechos de esta naturaleza, ejercer la acción penal contra los responsables criminales cuando tengamos pruebas suficientes para ello (y para eso intentar conseguir pruebas válidas

y útiles para acreditar los hechos) y defender los intereses y los derechos de las víctimas y, en general, de los perjudicados por este tipo de delitos.

A partir de este planteamiento es un honor informarles acerca de nuestra experiencia (llevamos trabajando como red aproximadamente año y medio) en aquellos delitos vinculados al uso de las TIC´s que más afectan a los menores de edad. Y de paso aprovecharé, si me lo permiten, para hacer algunas sugerencias de modificaciones legislativas en relación con este tema.

Indudablemente el primer aspecto que hay que abordar es el de los delitos contra la libertad e indemnidad sexual de los menores, dentro de los cuales es obligada la referencia a los delitos de pornografía infantil. Es esta una tipología delictiva que se ha visto extraordinariamente potenciada con el desarrollo de las tecnologías de la información y de la comunicación (también ocurre con los delitos de estafa, pero ello excede del área de trabajo de esta Ponencia). De hecho un porcentaje elevadísimo de las investigaciones que se incoan cada año por hechos asociados a la pornografía infantil son actividades ilícitas cometidas a través de estas tecnologías.

No me extenderé en cifras sobre la dimensión de este fenómeno, pues sus señorías contarán con información suficiente sobre ello, pero estimo de interés destacar que, según la Memoria de la Fiscalía General del Estado correspondiente al año 2011, un 12,52% de los procedimientos judiciales incoados en España por conductas asociadas al uso de las TICs tuvieron por objeto delitos de pornografía infantil y/o en relación con personas discapacitadas y el numero de acusaciones presentadas por el Ministerio Fiscal por hechos ilícitos de esta naturaleza se eleva a 368 en el mismo periodo anual.

Los tipos penales que sancionan los delitos de pornografía infantil están en permanente evolución porque todos los Estados están esforzándose

por adaptar sus legislaciones internas a una normativa internacional que, a su vez, también va avanzando a medida que la propia Comunidad Internacional toma conciencia del peligro que Internet supone, en la proliferación de estos ilícitos y en la expansión de sus efectos, en un ámbito en el que tan gravemente se ven afectados los derechos e intereses de los menores de edad. El esfuerzo de armonización normativa es especialmente importante dada la dimensión transnacional de estas conductas, lo que hace imprescindible que los Estados adopten una estrategia legislativa común para facilitar la cooperación en la investigación y enjuiciamiento de estos delitos.

Precisamente uno de los temas en que incide el Anteproyecto de reforma del Código Penal actualmente en curso es el relacionado con estás tipologías delictivas, que en su vigente regulación pueden verse afectadas en aspectos importantes, sobre los que estimo oportuno llamar la atención de sus señorías en atención a la función que posteriormente han de desempeñar en el proceso legislativo.

Consideramos importante y positivo que el borrador incluya en el Código Penal un concepto de pornografía infantil, hasta ahora no contemplado en nuestro ordenamiento jurídico. La razón de ello es que nos hallamos ante un materia que puede verse afectada, digamos, por matices de carácter ético, moral, religioso, de carácter ideológico. Y es bueno que la propia ley, el legislador, defina qué ha de entenderse por material pornográfico, por pornografía infantil, para así ganar seguridad jurídica y garantizar que todos los operadores dispongamos, al respecto, de una referencia perfectamente definida. Lo que hace el proyecto es tomar el concepto de pornografía infantil que se recoge en la Directiva 2011/92/UE, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil que, a su vez, hace suyo el que ya se contemplaba en la Convención de Budapest del Consejo de Europa.

Una segunda novedad destacable en el Anteproyecto es la tipificación como delito del acceso *on-line* a archivos con pornografía infantil. Permitan que me explique: en la actualidad en España son constitutivas de delito, y así se sancionan en el artículo 189 del código penal, no solamente las actividades de producción, fabricación, venta, exhibición, distribución y difusión de pornografía sino también la posesión de material de esta naturaleza para el propio consumo. La tipificación de esta última conducta, tal y como viene definida por el código penal y tal y como se está interpretando por los tribunales, requiere, para que pueda apreciarse la existencia de delito, que se haya producido no solo el acceso al material sino también la descarga efectiva y la posesión del mismo durante un cierto periodo de tiempo por parte de autor del hecho. Por el contrario no es delito, hoy por hoy, en nuestro país, el visionado *on-line*, lo que es conocido como *streaming*, de pornografía infantil, circunstancia que no deja de resultar una incoherencia en la medida en que actualmente el consumo de pornografía infantil generalmente se realiza *on-line* sin que lleguen a efectuarse descargas directas. Por otra parte es evidente que la lesión al bien jurídico protegido es muy similar en uno y otro caso, es decir en los supuestos de posesión para propio uso y los de visionado *on-line.*

En consecuencia el Anteproyecto opta por sancionar también esta conducta de acceso *on-line,* siguiendo también en este aspecto la Directiva antes citada del año 2011 de la Unión Europea, sobre explotación sexual de los menores y pornografía infantil.

Finalmente, y en relación con este mismo tema, destacaría una tercera aportación muy interesante del Anteproyecto que puede tener una gran eficacia. Me refiero al hecho de que se contemple expresamente en el Código Penal la posibilidad de que el juez, en el curso de un procedimiento criminal, acuerde el cierre de páginas web con contenidos de pornografía infantil cuando ello sea posible, por encontrarse ubicadas en servidores

radicados en nuestro país, o, en su caso, el bloqueo de la posibilidad de acceso desde España a estas páginas cuando las mismas se encuentren alojadas en servidores ubicados en otros Estados. La medida es importante para combatir este tipo de actividades ilícitas y en esa misma dirección apunta la última directiva europea. El Anteproyecto de reforma del Código Penal se refiere a la posibilidad de que el órgano judicial acuerde esas medidas con carácter definitivo, una vez dictada sentencia, y también, a petición del Ministerio Fiscal, con carácter cautelar, es decir antes de dictarse resolución sobre el fondo.

Actualmente estamos solicitando, y se están adoptando, medidas similares con apoyo en el artículo 13 de la Ley de .Enjuiciamiento Criminal y en los artículos 8 y 11 de la ley 34/2002 de servicios de la sociedad de la información y del comercio electrónico, pero es bueno que el Código Penal las contemple expresamente en su articulado, porque será una forma de potenciar el uso de las mismas y de soslayar cualquier duda acerca de su utilización.

En esta materia, relativa a los delitos contra la libertad e indemnidad sexual de los menores, es de interés la referencia a otro tipo de conductas, que desgraciadamente detectamos se están incrementando, y que son aquellas, vulgarmente conocidas como *child grooming*, en las que el agresor se aprovecha en general de las TIC y en particular de Internet para contactar con menores que no hayan alcanzado la edad para prestar el consentimiento para actos de contenido sexual y mantener con ellos una relación de esta naturaleza. Este comportamiento fue objeto de una tipificación específica en el artículo 183 bis del Código Penal, con ocasión de la reforma llevada a efecto por Ley Orgánica 5/2010 de 22 de junio, implementando en ese sentido la Convención de Lanzarote del Consejo de Europa.

Sin embargo, como ya alertó la Fiscalía General del Estado en su Memoria del año 2011, la rígida articulación de este tipo penal ha determinado que su aplicación práctica resulte escasa. La circunstancia de que el tipo penal contemple como victimas únicamente a los menores de 13 años (esto es porque en España actualmente la edad para prestar el consentimiento sexual está ahí, en los 13 años) y la exigencia de que la propuesta de mantener un encuentro con el niño deba acompañarse de actos *materiales encaminados al acercamiento* -que parece interpretarse como de carácter físico- limitan considerablemente la posibilidad de aplicación de este nuevo precepto. Como hemos podido constatar, en muchas ocasiones el autor de los hechos no pretende un encuentro físico con el menor, sino un encuentro virtual a los fines de lograr material pornográfico obtenido directamente o bien de inducir al menor a realizar ante la webcam actos de contenido sexual, circunstancia que determina que estas conducta -no incardinables, en principio, en este tipo- hayan de reconducirse, en su caso, a otros preceptos penales.

El Anteproyecto de reforma del Código Penal da respuesta a ambas limitaciones: por una parte eleva la edad de consentimiento sexual a los 15 años, lo que amplia el ámbito de aplicación de la norma en lo que se refiere a posibles victimas de estas actividades ilícitas. Esta medida, además, puede considerarse acertada porque España es, actualmente, uno de los países europeos que tiene fijado un límite de edad más bajo para prestar consentimiento sexual pues en los países de nuestro entorno el límite está en los 14, 15 e incluso 16 años, como es el caso el Reino Unido y Bélgica. Y por otra parte, y esta es la segunda aportación de la reforma, se tipifica también como delito esta misma conducta cuando el agresor no pretende el acercamiento físico sino la obtención de material pornográfico, con lo cual el nuevo texto saldrá al paso, si llega a ser aprobado, de los supuestos antes

referidos y que actualmente quedan al margen de la aplicación del artículo 183 bis del Código Penal.

Resta reflexionar sobre una cuestión que dejo para el análisis y valoración por parte de mi compañera doña Consuelo Madrigal: me refiero a los supuestos en los que el agresor es un menor de edad, es decir, cuando estas conductas se producen por parte de menores respecto de otros menores. Al respecto ha de recordarse que tanto la Convención de Lanzarote del Consejo de Europa como la Directiva del año 2011 de la Unión Europea, antes citada, circunscriben la persecución y sanción de estas conductas a los supuestos en que el agresor es una persona adulta que contacta con menores para este tipo de actos, no cuando los actores son también menores de edad.

Las actividades ilícitas vinculadas al uso de las TIC´s que afectan a los menores de edad no son solamente aquellas que atentan contra su libertad e indemnidad sexual sino que hay otro ámbito en el que la incidencia es también muy importante, concretamente el de los delitos contra la libertad, la intimidad y la seguridad. El incremento de las amenazas, coacciones, humillaciones y en general de los actos que suponen un trato degradante a menores a través de estas tecnologías es también llamativo. Y esta circunstancia es perfectamente lógica, porque los menores -y con esto me permito citar datos del Defensor del Menor de la Comunidad de Madrid, según los cuales un 90% de nuestros menores hacen uso con asiduidad de las redes sociales- utilizan esos mecanismos habitualmente para comunicarse entre si, por lo que están todo el día interactuando en el mundo virtual. Por ello canalizan también por esta misma vía este tipo de comportamientos de carácter injurioso, ofensivo o humillante, cuyos efectos además se agudizan por la capacidad expansiva de la red y porque al agresor le es más fácil actuar de esta forma más despersonalizada y que le ofrece cierta sensación de anonimato.

Hay muchas formas de agredir a un menor a través de estas tecnologías. Se pueden utilizar mensajes SMS de contenido humillante o degradante; puede elaborarse o poner en funcionamiento páginas web en las que posteriormente se vierten mensajes ridiculizantes o que ofenden al menor; puede suplantarse la identidad del menor y atribuyéndole determinadas manifestaciones o expresiones, perjudicar sus relaciones con terceros; es posible también grabar al menor en situaciones comprometidas o que ofenden su dignidad para difundirlas luego en las redes sociales, o por mensajes de teléfonos móviles, etc. Es decir, las acciones concretas susceptibles de lesionar los bienes jurídicos que nos ocupan pueden ser muy variadas.

El Ministerio Fiscal está persiguiendo, calificando y sancionando estas conductas en base a distintos tipos penales: como delitos de amenazas ó coacciones, delitos contra la intimidad, delitos de descubrimiento y revelación de secretos e incluso, en los casos más graves, como delitos contra la integridad moral. La casuística a la que nos enfrentamos es muy rica y variada por lo que es imprescindible atender a cada supuesto concreto para valorar cual es la tipificación más correcta en atención a la dinámica delictiva y a las circunstancias específicas de cada una de las conductas.

Y como, además, a medida que van avanzando las tecnologías se van produciendo variaciones en las manifestaciones criminales, en ocasiones se van generando zonas de impunidad, en el sentido de que van surgiendo nuevas conductas, cuya sanción no esta prevista penalmente pese a que son susceptibles de lesionar bienes jurídicos merecedores de protección y ello determina la necesidad de abordar modificaciones legislativas en el sentido antes indicado. Y al respecto estimo oportuno referirme a una conducta concreta que es la de la suplantación de identidad, que se está produciendo con relativa frecuencia entre adultos y también entre menores de edad y

que no tiene hasta el momento presente una respuesta especifica en vía penal. La Fiscalía General del Estado, en su Memoria del año 2011, alertó acerca de este comportamiento y abogó por su tipificación penal en determinadas circunstancias.

¿En qué consiste básicamente? Pues en suplantar la identidad de otro en todas sus comunicaciones *on-line* con carácter de permanencia y con unas connotaciones que aporten credibilidad, es decir, que la suplantación se haga en unas condiciones que induzcan realmente a error. Si se hace en esas condiciones esta conducta puede implicar un atentado grave contra la privacidad y puede tener una seria incidencia en las relaciones de la víctima con terceros en la medida en que permite atribuir, a aquella, opiniones, planteamientos ó manifestaciones que no son suyas y afectan a su consideración pública. Todo ello sin perjuicio de los efectos de esa suplantación cuando se realiza con fines criminales específicos.

En relación con los menores este tipo de conducta se está detectando en distintas manifestaciones. En ocasiones se utiliza para suplantarles y perjudicarles en su relación con terceros, es decir, el delincuente se interpone en el haz de relaciones del menor con amigos y conocidos generándole situaciones conflictivas con el grupo. En otros casos la suplantación tiene por objeto acceder a información ó a datos íntimos del menor. En este último caso cuando el atacante es una persona adulta la finalidad, normalmente, es obtener algún beneficio de carácter sexual y para ello se engaña al niño, haciéndole creer que el interlocutor es un amigo, para así conseguir de la victima el envío de fotografías o videos o que realice, o deje de realizar, determinadas conductas. De hecho muchos de los supuestos de acoso a menores a través de la red se llevan a efecto utilizando este tipo de engaño en las fases iniciales de la actividad ilícita.

Por todas estas razones el área de especialización en criminalidad informática ha abogado por la tipificación de estos comportamientos. En

relación con ello y como información complementaria parece oportuno comentar a sus señorías que algunos países, como Argentina y Perú, están trabajando en proyectos legislativos en esa misma dirección.

Y finalmente –cinco minutos y ya término– desearía hacer algunas aportaciones que considero importantes en el ámbito de la legislación procesal. Como les decía al principio nos encontramos con la circunstancia de que los instrumentos de investigación que tenemos legalmente articulados están pensados para ser utilizados ante una realidad delincuencial muy diferente a la que nos ocupa en este acto, ello hace que muchas veces estos instrumentos se nos queden cortos para investigar este tipo de actividades ilícitas, porque la tecnología ha ido proyectándose mucho más lejos.

Una de las figuras, por ejemplo, respecto de la que estamos percibiendo la necesidad de que sea objeto de una regulación complementaria, adaptada a la problemática que generan las investigaciones *on-line,* es la del agente encubierto. Es esta una técnica de investigación policial, regulada en el artículo 282 bis de la Ley de Enjuiciamiento Criminal, que está siendo muy útil en la lucha contra la delincuencia organizada pero que, en la normativa actualmente vigente, esta planteada en atención a las necesidades de actuación ante grupos criminales de carácter convencional y con existencia en la vida real (es decir, en la realidad física) y que se dedican a actividades ilícitas como el tráfico de drogas, el terrorismo o la trata de personas.

La experiencia práctica nos enseña que esta técnica podría ser muy efectiva en el ámbito de la investigación tecnológica. Así piensen, por ejemplo, en las conductas que hemos comentado de acoso a menores a través de la red y en las ventajas que podría ofrecer la posibilidad de utilizar un agente policial que pudiera hacerse pasar por el menor, -una vez iniciado el delito para evitar supuestos de provocación-, y de esta forma

facilitar la identificación del acosador. Sin embargo hay que admitir que la investigación *on-line* presenta peculiaridades propias que hacen que la normativa actual sobre esta materia resulte insuficiente a estos efectos.

A nuestro entender una regulación específica para esta materia habría de mantener las líneas básicas y esenciales de la figura, como son la exigencia de autorización judicial o del Ministerio Fiscal, dando cuenta de ello inmediatamente al juez; el control y seguimiento pleno y completo de la actuación del agente encubierto por parte del juez y la adecuación de la medida a criterios de necesidad y proporcionalidad, pues no hay que olvidar que no toda clase y categoría de delitos justifica el empleo de medios de investigación de esta naturaleza, ya que no se pueden matar moscas a cañonazos, permítanme la expresión. Pero sería necesario adaptar la normativa, en determinados aspectos, a las características de la investigación tecnológica.

Así, una primera dificultad que ofrece la actual regulación es que esta figura está planteada solamente para la investigación de determinados delitos y en todo caso en el marco de la delincuencia organizada. Al respecto hay que recodar en primer término que, en muchas ocasiones, las actividades ilícitas vinculadas al uso de las TIC´s nada tienen que ver con la delincuencia organizada sino que se presentan como actuaciones individuales e independientes unas de otras –insisto en la referencia a los acosadores de menores–. En segundo lugar, un buen número de los delitos enmarcables en el campo de la criminalidad informática no se encuentran incluidos en el listado del artículo 282 bis de la Ley de Enjuiciamiento Criminal, como es el caso de algunos de aquellos a los que me he referido anteriormente: las amenazas, las coacciones ó los delitos contra la integridad moral. Por ello sería bueno que se ampliaran las posibilidades de aplicación de esta figura a la generalidad de los delitos que se cometen a través de las TIC´s, sin renunciar en ningún caso –insisto en ello porque

esto es importante– ni a criterios de proporcionalidad, ni al debido control de la actuación del agente por parte de la autoridad judicial y del Ministerio Fiscal. Es decir, en la concesión de autorización habría de valorarse, en cada caso, la necesidad y la proporcionalidad en función de los bienes jurídicos que entren en conflicto.

Otra cuestión que plantea la utilización de esta figura, en las investigaciones *on-line*, es la de determinar el momento a partir del cual es preciso obtener autorización judicial para la utilización de una identidad supuesta y actuar como agente encubierto. En el entorno de la realidad física es para todos evidente cual es el momento en que un agente se introduce en un grupo de delincuentes -que le identifican físicamente- utilizando un nombre y apellido que no son los propios y que justifica generalmente con documentación identificativa preparada al efecto. Pero no puede obviarse, cuando nos referimos a la navegación *on-line* -no ya a la actividad delictiva- sino a la navegación *on-line* en términos generales, que es frecuente y habitual el uso de *nicknames* o identidades supuestas por la generalidad de los usuarios sin que ello genere preocupación alguna en los restantes internautas.

Por tanto habría que plantearse si es exigible autorización judicial para usar, en esos términos, una identidad supuesta, ó al menos que no es la propia, cuando el agente policial, en el ejercicio de sus funciones, está llevando a efecto una navegación libre por la red, es decir, cuando no busca un objetivo plenamente determinado, en atención a hechos y personas, sino que está accediendo a *sitios* de información pública. Cuestión distinta sería si la navegación tuviera como objetivo el acceso a foros concretos, cerrados, ó si la pretensión, al efectuar una *navegación encubierta*, fuera precisamente la de ocultar la cualidad de agente policial, a través de un engaño deliberado, o prolongar una investigación que en otras circunstancias no hubiera sido posible. En estos últimos casos parece

evidente la necesidad de autorización al juez. Lo que queremos poner de manifiesto es que esta es una materia que precisa de regulación específica en orden a establecer criterios acerca de las posibilidades de actuación policial en Internet utilizando *nicks* o identidades imaginarias o supuestas así como de las circunstancias que harían exigible autorización judicial para ello.

Finalmente he de referirme a la tercera de las cuestiones que se plantea en relación con esta materia, y que se centra en las posibilidades de actuación del agente encubierto en determinadas investigaciones. Es un hecho constatado que en ocasiones para acceder a determinados foros, y en concreto a foros muy restringidos como son los de fabricación de pornografía infantil o aquellos en que se están gestando y organizando ataques informáticos muy serios, es preciso que quien pretende ingresar de alguna manera demuestre una cierta sintonía con la actividad ilícita que ahí se desarrolla. Es una medida de seguridad que adoptan quienes participan directamente en estas actividades para evitar ser descubiertos. Y ello obliga a plantearse la conveniencia de regular la autorización por parte del órgano judicial, a quien vaya a actuar como agente encubierto, para realizar actos concretos que en sí mismos serían constitutivos de delito pero que resultan imprescindibles para acceder a esos foros y continuar la investigación iniciada. Es una materia que habría que ir abordando legalmente, valorando en que supuestos sería posible esta actuación, cual sería el alcance de la conducta autorizada así como la forma y garantías con que llevar a efecto el control judicial de esta actividad.

Otra modificación que estimamos de interés, y que no puedo dejar pasar la oportunidad de trasladar a sus señorías, se refiere a determinados aspectos de la ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación. Hay que recordar al respecto que en la investigación tecnológica el punto de

arranque de casi todas las indagaciones son los datos conservados por los operadores de servicios de comunicación pública, ya que, como bien saben, cada vez que accedemos a la red, o nos comunicamos a través del teléfono, el operador de comunicación pública que nos da la conexión registra y anota el dato de tráfico así generado. Esta información es esencial para averiguar, por ejemplo, quien ha proferido una amenaza a través de la red pues la determinación de la IP de conexión permite llegar a conocer, a partir de los datos almacenados, la procedencia de dicha amenaza y la identificación del autor.

La ley 25/2007 de 25 de octubre antes citada, que incorpora en España la Directiva 2006/24/CE, establece la obligación de los operadores de servicios de comunicación pública de conservar toda la información sobre datos de tráfico (no de contenido), generados por telefonía móvil, telefonía fija e Internet, durante un año, para tenerla –dice la ley– a disposición del órgano judicial que necesite usar de ella en investigaciones criminales –y aquí viene el problema– por delitos graves.

El concepto de delito grave puede entenderse en dos sentidos; en sentido estricto delito grave es aquel que está castigado con pena grave, es decir, superior a 5 años, bien de privación de libertad o bien de privación de derechos. Pero también puede asumirse un concepto más amplio de lo que es delito grave, entendido como aquel que afecta a bienes jurídicos muy trascendentes (como los que afectan a menores), ó los cometidos por organizaciones criminales, ó los que generan grave alarma social, con independencia de la pena que corresponda al delito. Tradicionalmente la Fiscalía ha venido sosteniendo, y así era asumido por los órganos judiciales, que la referencia a delito grave que se efectúa en el artículo 1º de la Ley 25/2007 había que interpretarla en sentido amplio y ello ha permitido acceder a los datos de tráfico de comunicaciones, conservados por los operadores, en las investigaciones de los delitos cometidos a través

de las TIC´s. Al respecto hay que recordar que casi todas las actividades ilícitas que han sido objeto de cometario en el curso de esta intervención son delitos menos graves y, por tanto, tienen prevista una sanción inferior al límite antes indicado.

Pero últimamente está tomando cuerpo una línea jurisprudencial que entiende que la expresión delito grave del artículo 1 de la Ley 25/2007 hay que interpretarla en sentido estricto, es decir, referida únicamente a delitos de pena superior a 5 años, lo que puede determinar que se cieguen las vías de investigación en muchos de estos casos.

La Fiscalía ya remitió hace varios meses al Ministerio de Justicia una propuesta de reforma legislativa, en la que trasladamos esta problemática y solicitamos la modificación, o, en su caso, la aclaración del concepto cuestionado en la Ley 25/2007, adecuándola al espíritu de la propia disposición legal y también al sentido de la Directiva del año 2006 y del resto de la normativa europea –como la Convención de Budapest del Consejo de Europa- que es el de potenciar la investigación de todos los delitos que se cometen a través de las TIC,s.

Aprovecho, por tanto la oportunidad que nos ofrece esta comparecencia para trasladar a sus Señorías nuestra preocupación por este tema, dado los problemas que se están generando en las investigaciones de esta naturaleza.

Y finalmente, no más de un minuto, en referencia a otro tema de especial interés relacionado con esta misma disposición legal. La norma que nos ocupa solamente obliga a los operadores de servicios de comunicación pública, no así a los restantes operadores, a los prestadores de servicios de Internet que sustentan las redes sociales. Esto genera un vacío legal y tal vez fuera conveniente abordar la regulación de las obligaciones que se estimaran oportunas sobre conservación de datos y facilitación de datos a las autoridades competentes por parte de todos los

prestadores de servicios de Internet, e incluso por parte de todas las personas físicas y jurídicas que realizan tratamiento de datos electrónicos, es decir, de datos derivados de estas tecnologías.

A ello se refiere específicamente la Convención de Budapest del Consejo de Europa sobre ciberdelincuencia que fue ratificada por España en el año 2010. Dicha Convención en su artículo 16 se refiere concretamente a ello, al instar a todos los países a regular legalmente la posibilidad de ordenar a cualquier operador de Internet la conservación de datos en supuestos determinados y su cesión a la autoridad competente cuando resulten necesarios en una investigación. En la legislación española todavía no se ha incorporado esta exigencia y sería bueno aprovechar las reflexiones que se están efectuando en este ámbito para abordar la implementación de la citada Convención en nuestra normativa interna.

Y nada más; lamento haberme alargado un poquito. Muchísimas gracias por su atención y quedo a su disposición.