COMPARECENCIA DEL COMISARIO JEFE DE LA BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA COMISARÍA GENERAL DE LA POLICÍA JUDICIAL DE LA DIRECCIÓN GENERAL DE LA POLICÍA, D. JUAN MIGUEL MANZANAS MANZANAS, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES EL DÍA 16 DE MAYO DE 2013.

El señor **JEFE DE LA BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA COMISARÍA GENERAL DE LA POLICÍA JUDICIAL DE LA DIRECCIÓN GENERAL DE LA POLICÍA** (D. Juan Miguel Manzanas Manzanas): (...) en primer lugar que mi intervención es la representación de un equipo de gente, como digo yo, de gente echada para adelante, profesionales comprometidos, con espíritu positivo y abierto, y que tengo la suerte y el lujo de dirigir.

Todos ustedes conocen personal o profesionalmente motivos de la importancia de las redes sociales como elemento de esta nueva revolución social y de su incidencia positiva, y a veces negativa, en la sociedad en general y los jóvenes en particular. La visión panorámica que les voy a relatar un poco, a exponer, está ubicada en ese tanto por ciento de utilización perversa de las nuevas tecnologías, vinculada con el delito, y por tanto menos agradable, pero en la que el Cuerpo Nacional de Policía tiene entre sus competencias la de identificar, localizar y detener a los autores de estos hechos delictivos.

La comúnmente conocida como BIT es la unidad que está encuadrada, como ha dicho el director general, dentro de la Comisaría General de Policía Judicial, en ese organigrama dentro de la Dirección General. Y su misión primordial, como el resto de unidades de Policía Judicial, es eminentemente

operativa, operativa y de investigación. Y está dirigida a la localización y detención de los autores de los hechos delictivos, es decir, una vez que se han cometido esos hechos, para ponerlos a disposición de la Fiscalía o de la autoridad judicial, proporcionando los medios de prueba necesarios para demostrar su culpabilidad o inocencia en los hechos.

De alguna forma, el origen de la BIT, de la comúnmente denominada BIT, se sitúa en torno al año 1995; lo hemos fijado en esa fecha porque es cuando se creó de alguna forma, por parte de un pequeño grupo de tres, cuatro personas, investigadores, que dentro de una entonces llamada Brigada de Delincuencia Económica y Fiscal, a esos pequeños delitos que tenían que ver de alguna forma con la parte informática o con más dificultades informáticas, dar una respuesta a los ataques y vulneraciones –en aquel momento– contra la piratería de software y determinadas estafas bancarias que se estaban produciendo en ese momento. Les hablo de unas fechas en las que, como ustedes recordarán, los sistemas operativos era el MS-DOS, los dispositivos de almacenamiento masivo eran los disquetes de 3½" y de 5¼", en fin, el acceso a las redes era impensable, lo que tenemos hoy en día. Esto, hablamos de 1995; a lo largo de ese tiempo se ha ido incrementando la actividad en ese área, paulatinamente, a la vez que se ha ido produciendo la nueva tecnología. Y en 2002 se conforma, se amplía, por decir así, el campo de actuación de ese pequeño grupo que se inició y se crea la Brigada de Investigación Tecnológica, la conocida BIT, hasta ahora. Ahí ya se incrementan una serie de actividades, entre las que ya tienen de una forma más consolidada la lucha contra la pornografía infantil y los abusos sexuales contra los menores, es decir, la protección contra el menor. Y el añadido, que es el motivo por el que inicialmente comenzó, algunas de las pequeñas estafas que se estaban produciendo por estos medios.

Es a partir de enero de este año precisamente, con la entrada en vigor de la orden ministerial a que ha hecho referencia el director cuando se pretende dar un

impulso, un reforzamiento de esta forma por parte del Cuerpo Nacional de Policía a la investigación en estos medios e incentivar de alguna forma, e incrementar la potencialidad de capacidades en este campo, creándose la Unidad de Investigación Tecnológica, que es sobre la que vamos a estar poniendo los pilares –esperamos– del futuro de esta línea de investigación.

El auge de las tecnologías de la información y la comunicación y la orientación de las nuevas formas delictivas en estos medios suponen un nuevo escenario que precisa una mayor respuesta en la investigación. Y para ello, en esta Unidad de Investigación Tecnológica, como antes ha mencionado el director también dentro de esta unidad, dentro de esta estructura, se creaban dos brigadas, con la finalidad de incrementar su actividad. Y además orientadas de una forma muy clara, precisamente para diferenciar las diferentes formas de actuación en la investigación, que implican, por un lado, los delitos que están relacionados con las personas, de lo que es la investigación de los delitos relacionados con los sistemas informáticos y con la red. La problemática es distinta; las formas de investigar son distintas; las formas de recibir las denuncias y los hechos también son muy distintos. Y esto nos obliga a actuar también de forma diferente.

En el ámbito de la investigación de los delitos contra las personas, lógicamente estaría integrada la protección al menor, la pornografía infantil, los delitos contra la libertad sexual, delitos contra el honor y la intimidad, las calumnias, injurias, redes sociales.

En esa otra brigada que está orientada a la investigación de los delitos contra los sistemas informáticos y la red es donde vamos a encuadrar toda esa actividad delictiva en el campo del cibercrimen que está vinculada con los delitos contra el patrimonio, en el que el objetivo principal es el ánimo de lucro inicialmente, aunque luego existen robos de información de datos, existen otra serie de delitos con carácter ideológico, de carácter de terrorismo, de espionaje

industrial, entre Estados, etc. Es una actividad que en una gran parte está orientada al campo de la actividad fraudulenta, a la obtención de un patrimonio, que es la más propiamente delictiva, hasta ir avanzando a una delincuencia de alta tecnología, por decir así. De hecho, esto es un poco lo que otros colegas a nivel europeo, por ejemplo los holandeses, que en un informe que han hecho de forma trianual, se puede ver que tienen la misma problemática; o sea, tenemos una situación de identidad en los problemas que tenemos, a pesar de que sean "holandeses", y que llevan más tiempo trabajando estos temas. Existe una identidad en sus conclusiones con la mayor parte de las problemáticas que tenemos. Esto no es un consuelo, pero es una forma de partida de que también estamos trabajando en ello. Y esta es la orientación que ellos han generalizado.

Dentro de esta investigación de lo que es la delincuencia de alta tecnología es donde tendremos un punto de colaboración con ese centro de respuesta y alerta temprana que se pretende crear dentro del Cuerpo Nacional de Policía, como se ha mencionado antes, y en el que intentaremos recoger todas las novedades y noticias que estén llegando de todos los países a nivel del cibercrimen, y colaboraciones directas con otras policías, no solamente del ámbito europeo sino del ámbito internacional americano, etc.

Esta organización de la unidad central potenciará igualmente nuestra labor de lo que comúnmente se conoce como BIT, que no es estrictamente este grupo de personas, sino que consta además de una estructura a nivel policial, como ustedes conocerán, a través de la Jefatura Superior de Policía, en cada comisaría provincial, en donde existe un pequeño grupo de personas que reciben las pequeñas denuncias, las pequeñas investigaciones más directas a lo mejor con el ciudadano, que unas son de pequeña actuación y otras tienen que ver en el contexto de un gran volumen de hechos o de daños que, generalizados, hay que coordinar desde la unidad central.

Y esa es la labor de la unidad, la de coordinación de toda esa actividad, a través también de esas pequeñas unidades que se creen a nivel periférico en cada comisaría provincial. Que además tienen que ser el soporte, y lo son de hecho, en el campo de las estafas, pero también, y lo están haciendo así, en el campo sobre todo de la pornografía infantil. Nuestra labor no es exclusivamente con los efectivos que tenemos, porque si no, sería imposible físicamente poder llevarlo a cabo, el nivel de detenidos que se hace al año en estos temas, y el nivel de operaciones que se están realizando, porque tenemos que contar con que se hacen operaciones simultáneamente en ocasiones de 10, 15 provincias, si no en el mismo día en días muy aproximados, y lógicamente, esto exige un nivel de respuesta coordinado con el resto de compañeros.

Hecho un poco este esbozo de lo que es la presentación de lo que va a ser la unidad, voy a intentar relatarles lo que son los campos de actuación, las áreas de intervención que hasta ahora estamos hablando, de lo que era esa Brigada de Investigación Tecnológica, con una infraestructura, con una estructura determinada. Hablaba antes de que inicialmente se creó con un grupo en el que los medios que se estaban utilizando eran los sistemas de almacenamiento de 3½"; en la etapa de 2002 hasta ahora estamos hablando de una etapa en la que la Brigada de Investigación Tecnológica estaba orientada fundamentalmente a la actividad de los delitos relacionados con la informática y en las redes, y esto suponía el estar orientada esa investigación a tener un terminal de un ordenador en casa, en el trabajo, en donde sea, en el que puedes estar conectado a la red. Es decir, tenías una identificación mediante una dirección IP que era la que te geolocalizaba, te identificaba, te situaba y te ubicaba en una zona.

Parece que esto se corresponde con esa nueva tendencia que se está produciendo en este campo, y es que hoy en día escasamente ya quedan ordenadores en casa, quiero decir ordenadores de sobremesa conectados a un punto fijo, y que todo se traslada a través de redes, redes WiFi, tabletas,

smartphones, telefonía móvil... Es decir, el punto de conexión con la red lo tiene cada individuo en su bolsillo en cualquier momento en cualquier zona del territorio nacional o extranjero. Esto cambia la dimensión de los parámetros que suponen para nosotros esos niveles de investigación y supone un reto añadido a esas dificultades que se van implementando. Es decir, es verdad que las nuevas tecnologías de la información y la comunicación van más deprisa que nosotros, afortunadamente también es un hecho interesante y bueno socialmente, y nosotros tenemos que ir con esos nuevos retos.

Para el Cuerpo Nacional de Policía constituye una de las prioridades todo lo relacionado con la protección del menor en el ámbito de las nuevas tecnologías e incidiendo especialmente en la lucha contra la explotación sexual infantil, participando en todo tipo de proyectos con las diferentes instituciones públicas y privadas, nacionales e internacionales, tanto universidades como ministerios, proveedores de servicios, etc. En la actualidad esta unidad está dimensionada con tres grupos operativos de protección al menor en los que se planifican operaciones encaminadas a la identificación y posterior detención de los usuarios de los programas de intercambio de ficheros a través de Internet, ya que constituyen la mayor fuente de victimización secundaria de los menores, circulando entre los pederastas las imágenes de los abusos de forma indefinida en el tiempo por Internet. Este es uno de los problemas que intentamos atajar.

Por eso la lucha contra la pornografía infantil abarca fundamentalmente dos aspectos: por un lado, trata de reducir en la medida de lo posible la cantidad de pornografía infantil disponible en la red. Así, intentamos luchar contra la red para intentar sacar toda la posibilidad de existencia de este tipo de imágenes. Y por otro, identificar a los agresores sexuales y sus víctimas.

No solamente hay que tener en cuenta esas imágenes y además las víctimas, sino que detrás de ellos existen unas etapas evolutivas de determinadas personas que no solo se benefician del comercio o lúdicamente de esas

imágenes, sino que además llegan a unos estadios en ese desarrollo, en esa evolución, en la que llegan a llegar al abuso, a la agresión sexual de esos menores. Y además con unas connotaciones francamente aberrantes. Hablábamos esta mañana de una de las operaciones que se han dado a conocer –Carolina seguramente... lo hemos estado hablando–, y resultan francamente difíciles, con menores de dos años con determinadas agresiones. Resulta francamente difícil.

Traía una serie de operaciones especificas para relatarles pero no les quiero cansar con estas cosas, voy a hablarles de cuestiones más generales.

Una de las implicaciones más importantes de esta área de protección al menor, necesariamente es la formación. Los especialistas no solo están especializados en investigación de policía judicial, sino que además tienen que reunir una serie de conocimientos específicos necesarios, de tipo informático, a veces un poco más friqui, como solemos decir nosotros, pero es verdad que tienen que estar ahí; hay que estar despiertos, hay que estar abiertos, son gente lista.

Entonces, ¿por qué? Porque cuando se interviene en cualquier tipo de operación tenemos que pensar en la otra parte de lo que es nuestro fin, no solamente detener a esa persona, sino buscar esas evidencias electrónicas que tenemos que proporcionar a la autoridad judicial. Y eso es un problema que tiene la policía en general, y en este caso nosotros en particular, porque la verdad es que proporcionar o conseguir ese tipo de evidencias cuesta; cuesta y hay que conocer los entresijos de verdaderos especialistas y técnicos que hay en estos temas a nivel de usuario, a veces elemental; cualquier chaval hoy en día, son superavezados y llegan a conseguir auténticas maravillas.

Esto implica una serie de actividad de mejora permanente en el propio policía a través de formación no solamente nacional, sino con empresas privadas, a nivel internacional. Estamos acudiendo a cualquier grupo de trabajo

o país que está incorporando cualquier novedad sobre estos temas, e incluso, es verdad, nos procuramos arrimar mucho a algunas empresas privadas, por ejemplo de antivirus, etc., porque en ese contacto con ellos también existen, se generan unos círculos de confianza que nos proporcionan, por un lado, esos conocimientos que ellos tienen sobre las maldades que se pueden llegar a detectar, y nosotros la forma en que se están produciendo para poder intervenir. Es una especie de mutua colaboración.

Quiero significar una cosa muy importante en esta área de protección al menor: y es que las personas que están aquí dedicadas tienen –cómo les diría–, se encuentran sometidas a una presión especial. Quiero decir, que estar viendo y buscando determinadas imágenes de este tipo tan aberrantes supone a veces, depende de cada persona y su situación, personal, familiar y demas, puede suponer una carga importante.

En otros países, como aquí también, hemos tenido ocasiones en que alguna vez que buenos profesionales, buenos policías hemos tenido que sacarlos porque podían llegar a tener problemas incluso psicológicos. De hecho, en algunas unidades policiales del centro de Europa existe más o menos una... se van haciendo unos exámenes, incluso test psicológicos, y a lo mejor a los dos años o tres años, cuando se ve necesario, se les traslada a otras unidades, a otros grupos para que cambien, porque realmente el permanecer mucho tiempo viendo esto puede perjudicar, “por muy buena pasta que se tenga”. Esto quería que quedara claro, porque aparentemente pasa desapercibido, nadie lo ve, pero cuando se ven determinadas imágenes, si se ven permanentemente y tan diferentes, llega a suponer una carga importante.

Quiero hablarles un poco del ámbito de colaboración precisamente que se produce en este campo de la pornografía, de protección del menor. El ámbito de colaboración en diferentes frentes: en el ámbito internacional, yo creo que el volumen de actividad o de colaboración en el ámbito internacional es el mayor,

es decir, el estar permanentemente en los grupos de trabajo de Interpol y de Europol y en permanente contacto con las policías de todos esos países, y las bases de datos que se generan sobre pornografía infantil, son los que mantienen el volumen de operatividad y a veces y, seguramente también, el nivel de eficacia que se tiene, en general creo que va correlacionado.

Este nivel de colaboración es tan puntual que se mantiene permanentemente a lo largo del día en contacto con cualquier policía: de Finlandia, de Suecia, de Alemania, etc. de modo que en cualquier momento nos comunican determinada imagen que han visto, nos lo trasladan porque creen que ese tipo de imagen puede estar orientada en una zona, una región de España; lo vemos, y entonces empiezan a sacarse conclusiones sobre determinados objetos o determinadas situaciones, y se empieza a intentar geolocalizar esa imagen, etc. Esa relación con todas esas policías es la que genera una actividad mayor potencialmente, y es la que, digamos, nos está llevando un poco en volandas en este campo. El entendimiento es increíble. Además la colaboración en este campo es muy buena. Independientemente de que por nuestra parte también estamos rastreando cualquier imagen en lo que es el entorno a nivel nacional. Y las denuncias, lógicamente, que se producen a través de los propios ciudadanos en las comisarías, y también en gran medida de las denuncias a través de las redes sociales que tenemos en la dirección y de la página web. Es una fuente importante que nos permite estar muy en contacto con la realidad puntualmente, y a cada víctima la podemos ir tratando según la situación en la que psicológicamente puede llegar a encontrarse, que esto también es importante en este caso.

El nivel de colaboración, ya digo, en el campo de las nuevas tecnologías, tanto en Interpol como en Europol, he señalado aquí algunos de los grupos en los que se interviene: el Grupo Europeo de Nuevas Tecnologías de Interpol, en el Grupo Latinoamericano también de Interpol, en la lista 24/7 de Interpol,

proyecto CES(?), proyecto CIRCAMP, en fin, la *Virtual Global Task Force*, una serie de grupos, en los que además cada uno de los jefes de grupo está asignado, acuden permanentemente de forma regular. Cuando aparece una operación se convoca y asiste cada uno de los jefes de grupo en Bruselas, en Lyon, etc., y se generan unas pautas de trabajo que en cada unidad policial a nivel nacional luego se va aportando lo que en definitiva se va trasladando en cada país. Hay algunas operaciones en este sentido, no solamente en el campo de Europol e Interpol, por ejemplo la operación "Espada", que procedía de una información que nos vino a través de Toronto en Canadá, supuso del orden de 56 detenidos aproximadamente, que se llevó a cabo y que fuimos el país que más actividad desarrollamos en la identificación incluso de las víctimas, y en ese caso la verdad es que tuvimos la suerte de que la propia policía canadiense nos felicitó y quieren que asistamos cuando el resto de países haya finalizado cada una de sus operaciones a nivel internacional, para que compartamos esa rueda de prensa o puesta de largo de finalización de esa operación, en la que también Estados Unidos tuvo una parte importante.

Preguntaron ustedes cuando estaba el director sobre el tema de la prevención: nosotros somos una unidad eminentemente operativa, de investigación. Pero el campo de la prevención tampoco lo hemos desechado, es decir, aunque la tarea policial de lo que es la prevención la lleva Seguridad Ciudadana, y también la tarea de la prevención en el campo de las redes sociales fundamentalmente lo lleva Carolina, que ya les indicará algunas cuestiones más nosotros, no obstante, siempre que hemos realizado cualquier operación, en base a la experiencia que hemos ido teniendo hemos introducido algunas pautas, comentarios, sugerencias que luego en prensa se han ido recogiendo al finalizar cada operación, para que los usuarios y cualquier persona lo tengan en cuenta.

Pero no solamente hemos dado esas líneas de prevención, sino que además colaboramos precisamente con esta unidad provincial que digo que es de

seguridad ciudadana, a través de la Unidad Central de Participación y Programas. Esa una unidad dedicada especialmente, dentro del campo de la seguridad ciudadana a nivel nacional, en todas las capitales de provincia, donde existe un delegado provincial de participación ciudadana, que es el interlocutor con todos los grupos sociales locales, a nivel provincial, etc., que son los que intervienen y dan charlas, tanto programas del tipo "Policía-escuela", "Mayores", "Violencia de género", etc.. Precisamente a ellos es a los que les proporcionamos la formación y la información para que luego puedan trasladarlo a nivel nacional. Y ellos son los que luego a nivel nacional participan regularmente, unas veces a petición y otras veces de forma oficial, por nuestra parte en los colegios, en las escuelas, en los institutos, haciendo algunas indicaciones sobre todo esto.

Además en muchas ocasiones, por otras circunstancias también hemos sido requeridos expresamente para participar y lo hemos hecho así, sobre todo y principalmente, como es lógico, a este sector de clientes que son los menores y en temas de redes sociales.

Otro de los ámbitos de colaboración que se planteaba, y que ha sido también objeto de una pregunta, es la colaboración con el sector público y el sector privado. Hay una importante colaboración, sobre todo aquí, con las ONG (Protégeles, Save the Children, etc.); son, digamos, una parte importante para nosotros, y ellos también lo entienden así con nosotros. Es decir, hay una comunicación muy buena, muy cordial, muy fluida, el entendimiento es permanente; proporcionamos y nos proporcionan un *feedback* muy importante de lo que sucede, de lo que está sucediendo, e incluso nos trasladan gran parte de las denuncias. Y esa parte previa a la denuncia que representa ese choque para el que está sufriendo ese ataque, ese acoso o esa situación, el canalizarla muchas veces a través de esas ONG facilita esa preparación previa para que luego podamos intervenir. Y la verdad es que en este campo, en este sentido la

colaboración es estupenda y creo que muchas veces es bastante patente y muy satisfactorio para ambas partes. La verdad es que es una de las cuestiones más agradables dentro de todo esto por la buena sintonía que hay y por la afinidad en ese entendimiento.

Otras cuestiones motivo de colaboración: en proyectos de investigación, de I+D. Precisamente desde la brigada, desde hace año y medio, va a hacer casi dos años, se está llevando a cabo un proyecto a través de subvención de la Comisión Europea en el que estamos participando, poniendo, por decir así, en valor la experiencia y el conocimiento que tenemos para conseguir unas herramientas que nos faciliten y mejoren el trabajo a la hora de intervenir el material informático que recogemos en las intervenciones, en las entradas y registros, y que todo ello además nos sirva de filtro y que nos genere procesos automáticos que nos facilite la recogida de evidencias electrónicas para luego aportarlas con las mejores garantías a la Fiscalía y a la autoridad judicial. Y cuando digo “con las mejores garantías”, hablo de intentar introducir cada vez más y de la mejor manera posible esa cadena de custodia que muchas veces no sabemos cómo hilvanar en este campo de la actividad de la red, de los delitos informáticos. Porque no sabemos muchas veces cómo tratar, o nuestros interlocutores, a veces los jueces, los fiscales y demas, no saben percibir en ese mundo físico y virtual en el que nos encontramos cómo detectar. Una evidencia física en un asesinato de una persona mediante un cuchillo la evidencia es palpable: el cuchillo. Aquí (en internet) una evidencia es algo abstracto que no aparece en ningún sitio, que yo digo a veces que implica un efecto de acto de fe por los jueces, aunque nuestros atestados y nuestra cercanía permanente con ellos para intentar aclararles cómo es, cómo se produce, dónde está, por qué es así, la verdad es que ellos también ponen una parte importante en ese esfuerzo para poder conseguirlo.

Como decía, este proyecto de colaboración se está llevando a cabo con el Instituto de Telecomunicaciones de la Secretaría de Estado de Telecomunicaciones está bastante avanzado el proyecto. El otro día estuvimos precisamente en León, en su sede, y ya está hecha la maqueta, estamos en un momento en el que se va a intentar introducir la prueba piloto para ver cómo se empieza a desarrollar, y creo que puede ser una de las herramientas que no solamente a nivel nacional, sin que incluso –y esto puede ser muy bueno a nivel nacional– puede ser vendible, es decir, no de la imagen de la propia policía, sino de España, en otras policías a nivel europeo e internacional.

Por la experiencia, porque ha sido realizado íntegramente por gente que está trabajando permanentemente en esto, en razón a sus necesidades y con la buena predisposición de los mejores técnicos e informáticos y desarrolladores de estas aplicaciones. Espero que esa herramienta nos dure mucho tiempo, que no se nos quede desfasada en poco tiempo, que es el problema a veces de estas situaciones. Pero creemos que vamos a conseguir un producto que por lo menos nos va a dar unas bases muy consistentes en la investigación, facilitarnos mucho las tareas y sobre todo a nivel judicial, porque vamos a poder integrar en ese sistema de gestión de evidencias, que además le va a proporcionar una mayor garantía, seguridad y tranquilidad a la Fiscalía y a la autoridad judicial, con la que precisamente, si conocen en nuestro ámbito, la Fiscalía especial contra la criminalidad informática, con Elvira Tejada, con la que por supuesto estamos en permanente contacto y comunicación en este sentido.

Cómo no, la colaboración con las empresas prestadoras de servicios, especialmente de redes sociales: también ha sido objeto de una de las preguntas. Creo que puedo contestarles con ello también a una parte, y otra parte seguramente se lo va a contestar en su discurso Carolina. Nuestra función primordial es la de investigación, el contacto con los operadores y con las empresas prestadoras de servicios de redes sociales. Nuestro caso es orientado a

recabar la información, los datos sobre el momento en que se ha producido el hecho, el delito. Creo que la situación el director la ha perfilado perfectamente: es verdad que es difícil porque muchas de estas empresas (menos alguna que está en España, lógicamente), están todas situadas en países extranjeros, en los que no se percibe de idéntica forma esa situación en la que los datos, dependiendo de cuál sea el delito, la consideración que tiene ese delito, o la interpretación y las costumbres de ese país que puedan hacerse de ese delito puedan facilitar en mayor o menor medida la informacion y los datos. Esto realmente supone un problema importante para nosotros en la investigación, sobre todo en algunos delitos vinculados a calumnias, injurias, sobre todo en personas mayores de edad.

Sin embargo, tengo que decir también que en el campo de la pornografía infantil, en el de la protección del menor suelen ser bastante sensibles, suelen participar mucho, e incluso nos suelen proporcionar esa información con mucha más facilidad, con mucha más asiduidad, incluso sin recabar el correspondiente mandamiento judicial, porque parece que es un delito universal en todos los países y se entiende muy bien esa problemática y todo el mundo colabora. Es una forma, yo creo que es la forma más fácil y en la que todo el mundo lucha más desinteresadamente en todo el ámbito internacional.

No quiero hablarles ya de lo que es el acoso sexual a los menores, el *grooming*, les ha mencionado también el director, también el *cyberbullying*, el acoso escolar a través de medios como el YouTube y demás. Seguramente también tiene que ver un poco lo que vayan a percibir cuando Carolina les haga la mención sobre redes sociales.

Lo que sí quiero trasladarles es la idea de la mayor utilización de los *smartphones* hoy en día. Es nuevo reto que se nos está planteando, es una nueva dimensión de lo que implica esto en el campo del crimen dentro de las tecnologías de la información y la comunicación, es un elemento de una difusión

muy rápida, muy eficaz, exponencialmente de forma geométrica, y que el pequeño detalle que pueda suponer una difusión a un amigo, a un tercero de una determinada imagen puede representar un daño brutal a nivel de la víctima.

Un poco derivado por la fluidez y la agilidad de lo que puede suponer en la red, y que además, como se suele decir, todo lo que entra en Internet se queda en la red. Eso es un problema que está ahí y con el que tenemos que luchar.

El campo de las injurias y calumnias y amenazas tiene su problemática, y además importante. El gran crecimiento que ha experimentado tanto el uso de los *smartphones* como de las redes sociales, gracias a la expansión de las conexiones móviles, está propiciando un notable auge de los delitos contra las personas en lo referente a las calumnias e injurias, así como contra la intimidad. Todo ello queda reflejado en el aumento de las querellas y denuncias por estos delitos, ya sea contra particulares, personajes públicos, políticos, empresas, etc. Parece que existe esa anonimización, ese anonimato que genera el estar dentro de la red, las posibilidades de anonimizarse por parte del que produce esas injurias y esas calumnias hacen desinhibir muchos principios, incluso sociales o fomentarlos y sacarlos fuera a través de la red, con el problema o el perjuicio que ello ocasiona a todas esas personas.

Es un problema realmente importante, vinculado también precisamente con las empresas que prestan esos servicios: el que exista esa dicotomía a la hora de trasladar o de facilitar esos datos para poder intervenir en nuestro caso. Hay que tener en cuenta que este tipo de delitos son delitos semipúblicos en los que interviene mucho la consideración de la posible injuria; hay ocasiones en las que son muy evidentes, muy claras, auténticas barbaridades atroces; otras en las que puede estar rayando la interpretación o el pequeño... la intuición, un trasfondo detrás de ese mensaje que puede generar psicológicamente esa duda, esa inseguridad, ese problema a esa persona.

Este tipo de delitos, realmente tiene escasa penalidad, seguramente porque tiene que ser así, no lo sé, pero eso también motiva el que en muchas ocasiones nuestra intervención a la hora de judicializar cualquier intervención de este tipo, la propia autoridad judicial define si considerarlo como delito o sobreseerlo porque no ve realmente que en ese mensaje pueda llegar a interpretarse de esa forma (sin embargo, para la víctima sí); o incluso que pueda derivarlo a un enjuiciamiento por faltas. Esto es, que procedimiento se debe seguir.

Pero nuestra intervención para llegar a conseguir esos datos implica que para poder llegar a determinar –si es que se puede llegar a determinar– la identidad de esa persona, tendríamos que recavarlo a través de esas empresas de servicios, seguramente de servidores extranjeros, y además mediante una comisión rogatoria internacional. Claro, esto, pensando en la consideración del delito, etc., llega muchas veces a dificultar tanto que realmente resulta más que dificultoso el éxito de la investigación. Es realmente un problema añadido y una cierta inseguridad en la víctima, eso sí es verdad.

No obstante, intentamos alertar a los usuarios en este sentido, de alguna forma para evitar esos enlaces, llegar a cerrar, o para evitar ese ciberacoso que puede haber, y hacemos un seguimiento para que en cualquier atisbo de que pueda desviarse o de que pueda incurrir en algún fallo esa persona, ese delincuente, poder identificarlo.

Algunas de estas empresas de servicios proporcionan algunos mecanismos a la hora de investigar dichos delitos. El poder identificar, como he dicho, a la persona que realiza los hechos teniendo como único dato un correo electrónico o solamente un *nick* o seudónimo, como ocurre en la red social Twitter, ya que en la mayoría de las ocasiones estas empresas tienen ubicado el domicilio social en el extranjero y estando sujetas a las disposiciones legales de esos terceros países no ofrecen ningún tipo de dato para la identificación de sus clientes.

Quiero incluir en ese otra área de la Unidad que inicialmente he mencionado, que está orientada a la investigación de los sistemas informáticos y la red por la importancia que tiene en los delitos vinculados con las estafas, los fraudes, etc. Porque aparentemente son una serie de delitos de pequeña cuantía, pero que potencialmente generan un daño social importante por su expansión, por su atomización.

La estafa, en cualquiera de las manifestaciones, constituye la actividad más lucrativa y menos punitiva individualmente, y hacia la que se encamina el resto de las actividades cibernéticas en general. Por lo que los sistemas de ocultación o navegación anónima y suplantación de identidad, para no ser identificados los autores y los grupos delictivos, son cada vez más sofisticados y complejos de investigar.

Cuando hablábamos de que inicialmente, cuando se creaba la Brigada, hubo un pequeño grupo que se encargaba de investigar estas pequeñas estafas estábamos hablando de estafas que eran trasladar aquellos timos antiguos del tocomocho, etc., que se producían en el nivel físico, trasladarlos a un entorno de la red; hoy en día están alcanzando un grado mucho más complejo, mucho más elevado, de tal forma que eso es lo que ha dado lugar a que creemos un área de investigación más potente que es el de seguridad lógica.

Porque precisamente existe un campo de estas estafas que está vinculado a una serie de actividad delictiva con determinados grupos que realizan estafas a través de transferencias electrónicas fraudulentas, el denominado *phishing* bancario, que ha sido tradicionalmente conocido por todo el mundo, el *pharming*, etc., o a través de ventas y subastas ilícitas en Internet o ventas y subastas también fraudulentas de artículos que luego revenden, etc.

Digamos que todo este campo más tradicional de las estafas, de los fraudes está llegando a tener un componente todavía mayor a la hora de que, para llegar a estafar, lo que se hace es lanzar en la red, así sin más, un cartucho:

ese cartucho va por la red como Pedro por su casa porque se lo permiten determinados ordenadores llamados zombis, de los que podemos tener uno en casa y no lo sabemos, y que nos lo están utilizando, a través de determinados servidores que anonimizan la autoría, la entrada y salida de quien lo está realizando.

Realmente son auténticos cartuchos explosivos que, llegados a un usuario final, le proporcionan el virus que va a originar cualquier tipo de actividad fraudulenta, ya sea cualquier tipo de estafa, ya sea recoger datos o información de nuestros propios ordenadores, utilizar nuestro propio ordenador como un *botnet* más para utilizar sus medidas, etc.

Estoy hablando a nivel particular, esto es, sin tener en cuenta que a nivel empresarial, es decir, a nivel de la pequeña y mediana empresa, que también tienen sus pequeños servidores domésticos a veces, pequeñas empresas de 8 o 10 personas con sus dos o tres ordenadores para gestionar su pequeña contabilidad, su pequeño negocio, etc., pues lógicamente ahí el daño todavía adquiere una dimensión mayor.

No digamos si esto se hace a nivel de las grandes empresas, incluso empresas nacionales o multinacionales, tanto españolas como extranjeras, en las que esto puede suponer una auténtica bomba en sus sistemas de seguridad lógica y repercutir gravemente en la seguridad de su información, a nivel de usuarios, de sus clientes, seguridad en sus sistemas, seguridad de espionaje en su propia red, y que luego van a vender a otra empresa de su competencia. Es decir, entramos en un mundo un poco mucho más complejo.

E incluso, dentro ya de ese grado más, el que todos consideramos en llamar de las infraestructuras críticas, con lo que representa y puede perjudicar a nivel nacional en cualquier Estado cualquier fallo de seguridad en estos sistemas.

Hasta el día de hoy teníamos esa tendencia a considerar las infraestructuras críticas, y orientar la seguridad de éstas en la seguridad privada, de esas grandes centrales nucleares, de esa subestación eléctrica, etc.; realmente el esfuerzo en seguridad privada que han hecho esas empresas es grande, pero es verdad que los problemas realmente y potencialmente más graves y que pueden perjudicar no solamente a los usuarios sino al funcionamiento de los sistemas, en la vida normal en un país pasan por estas grandes empresas, por eso son de infraestructuras críticas, y cualquier daño que se les pueda producir puede repercutir muy gravemente en la sociedad.

No voy a extenderme mucho en el tema de los fraudes, no quiero cansarles. La gente que estaba conmigo, todo el mundo quería aportar sus cosas, sus ideas, (todo el mundo quiere meter sus cosas); no quiero cansarles con todo ello.

Sí que es verdad que al hilo de lo que les estaba diciendo en el tema de este tipo de fraudes y de estafas, hay sector que es en el que estamos trabajando, en esas estafas de *phishing* que todavía siguen llegando, ahora mucho más sofisticadas. Antes el *phishing* llegaba porque te plantaban una página web que te pedían tus datos de códigos y contraseñas de determinada entidad bancaria en la que de modo *online* estabas trabajando; hoy en día, todo esto se traslada al uso de la tecnología móvil, en la que además de esas medidas de seguridad las entidades bancarias te permiten que si quieres hacer cualquier operación, o transferencia te van a enviar un mensaje a tu teléfono móvil para darte un código que puedes introducir, y así garantizar que tienes esa seguridad en la trasferencia; pues esto también ya lo han conseguido. Es decir, el que estén utilizando a su vez no solamente esa contraseña, perciben cuál es tu teléfono, te mandan un mensaje a tu teléfono y te indican que el banco con el que estás operando, supuestamente, te va a dar este archivo para que de forma encriptada puedas hacer estos mensajes con total garantía y con total seguridad.

Ese es justo el momento en el que se ejecuta un pequeño virus que te están mandando a tu teléfono móvil, fundamentalmente a los *smartphones*, seguramente porque es el tipo de telefonía más extendido en la mayor parte de la población hoy en día, sin descontar cualquier otro tipo; y a partir de ahí conocen tus datos, tus claves, tienen secuestrado tu teléfono, de tal forma que entran, ven tus cuentas, tus líneas, y si tienen que hacer cualquier transferencia lo van a estar derivando a través de ese teléfono móvil que ellos van a encontrar para hacer la transferencia, la operación, sin que tú te des cuenta. Esto es así.

Es verdad que operan con mucha rapidez, tienen mucha agilidad. Además, cuando lo hacen, lógicamente lo hacen mediante unas líneas de telefonía móvil, de mensajería, que acuden a unos servidores –nosotros tenemos detectado uno ahí en el norte de Europa– en los que a su vez redirige esos sistemas de mensajería, con lo cual resulta poco menos que difícil o imposible. Entramos ya en la dinámica de tener que acudir al exterior para poder lograr identificar a esa posible persona. Con la dificultad también añadida de que puede estar en un correo electrónico, en fin, no quiero...

Esta es una de las últimas, no sé si novedades o tendencias, en la que por supuesto tenemos una investigación pendiente que nos está llevando tiempo pero que está trasladando una parte importante de nuestra actividad. Y precisamente es una de las líneas que tenemos que empezar a orientar con más potencialidad y en la que necesitamos más ayudas, que tenemos que ir buscando, y formación que tendremos que ir proporcionando. Y es en el uso de la telefonía móvil, como elemento, ya digo, de integración del acceso a la red de cualquier persona. Es uno de los problemas realmente importantes.

Bien, en el campo de las ventas y subastas fraudulentas, esto ya es un poco, si se quiere, más doméstico. Mediante correos *spams* te recibes un correo en el que te... o a través de alguna página web en la que se vende cualquier artículo, aquí hablamos de los estafadores de temporada; es decir, cuando la

mayoría de la gente tiene que buscar un apartamento para ir a la playa en verano, pues se produce un movimiento de búsqueda de ese tipo de páginas en las que queremos buscar un apartamento en determinadas zonas para alquilar. Ese es el momento idóneo para poner ese tipo de anuncios de alquiler de apartamentos falso. Cuando pasa el verano, pues de apartamentos para los estudiantes para la universidad, cuando llegan las Navidades, de artículos de electrodomésticos, de bicicletas, de ordenadores, etc. Esta es un poco la secuencia.

No voy a extenderme mucho más, porque sí quería indicarles la tendencia o la orientación que vamos teniendo en el área de seguridad lógica, y en la que seguramente las investigaciones son más difíciles, son más costosas de tiempo y de esfuerzo, en la que tenemos gente preparada y muy espabilada, en la que tenemos una gran fuente y una gran conexión y apoyo con las policías internacionales porque si no, de otra forma tampoco sería posible, que es en el tema de seguridad lógica.

Ha mencionado el director algunas de las operaciones en las que hemos intervenido: una de ellas, la detención en Navidades precisamente de la persona responsable de lo que es la organización criminal más importante que estaba originando uno de los mayores problemas de seguridad y de estafa en la red, que es la operación "Ransomware"; una persona, un ruso que desde Rusia estaba lanzando una serie de mensajes mediante página web que en cada país se determinaba un anuncio en que conminaba al usuario en particular a pagar una multa por haber entrado, supuestamente, en algunas páginas de contenido no deseado, ya sea de pornografía infantil, de juego *online*, etc., y por las que debíamos pagar una multa.

Esto es falso, hemos dado recomendaciones sobre esto permanentemente, e incluso a través de Inteco se realizó un pequeño software para que todos los usuarios acudieran y desinfectaran su ordenador de este virus. Pero esta gente aprende. Y estos virus los reciclan, los cambian. Esto le llegó a pasar hasta a mi

hijo, que me dice “me ha pasado el virus este, pero es que además estoy saliendo en una ventanita por la pantalla”. O sea, llega un momento en que no solamente te introducen el virus en el ordenador, sino que acceden a tu cámara web y desde ahí la activan y te encuentras con la sorpresa de que te estás viendo incluso allí mismo. Esto a cualquier usuario, no solo le sorprende, sino que le invade de inseguridad.

Esta línea es la que nos ha obligado a trabajar en que no solamente tenemos que trabajar en verificar quiénes son los que estaban introduciendo los códigos para introducir este virus a nivel internacional; hemos tratado con cerca de diez o doce países en el ámbito europeo a través de grupos de trabajo de Europol, en los que además se les ha participado cómo se trabajaba y en los que ellos también están trabajando cada uno en sus países.

Potencialmente el que más daños –creemos, o porque lo ha contabilizado así– ha sido Alemania, pero también una parte importante en Estados Unidos, en la que a través del FBI se les ha proporcionado una parte importante de lo que es la organización, que la están explotando a su manera, de otra forma, están sacando mucho más partido seguramente por la idiosincrasia, las formas procedimentales y judiciales que existen allí, etc.

La investigación no solamente era buscar, localizar e identificar a estas personas, sino además qué es lo que pasaba con ese daño patrimonial que se estaba causando a los usuarios. Es decir, por un lado existía la rama técnica, que era esta; por otro lado la rama patrimonial.

Es decir, una vez que se producía el daño y la persona pagaba, mediante unos medios de pago en *Ukash*, o *paysavecard*, que simplemente se pueden adquirir en una gasolinera, (pagas 100 euros y es un cheque al portador), metes esos códigos en Internet y ya has pagado.

Tenían sus propios paneles de pago e inmediatamente detectaban que ya habías pagado y te liberaban el ordenador: tal cual.

Ahora viene la segunda parte, cómo recoger el fruto del delito. Y ahí entraba toda esa secuencia de forma de blanqueo en el que actúan en cada uno de los países. En todos los países tenían alguna de las células que se dedicaban a blanquear, mediante diferentes sistemas, bien a través de mulas, lo pasaban en efectivo, lo metían a través de locutorios, lo reenviaban a través de Western Union o Money Gram: un auténtico laberinto de ingeniería que nos ha supuesto mucho esfuerzo verificar, hasta llegar, por supuesto, que el dinero llegase a Rusia en este caso.

Por eso el trabajo que estamos dedicándole a la estafa se nos está identificando con toda esta problemática de estos sistemas.

Quiero decir que la colaboración internacional es tan grande en este sentido, que incluso estamos participando, como ha señalado también el director recientemente, en grandes operaciones. En Semana Santa se produjo uno de los mayores ataques de denegación de servicio, DDoS, en la red a través de Internet, a través de grandes empresas, una alemana, una holandesa y demás, que realmente no bloquearon la red a nivel internacional pero sí la saturaron de tal forma que hubo bastantes problemas, sobre todo en Estados Unidos, Inglaterra, Alemania y Holanda, incluso Suiza.

En esos dos o tres días, la comunicación, el contacto, el conocimiento entre profesionales de policía de diferentes países nos llevó a que se pusieron en contacto entre ellos. Nos comentaron cuál era la situación, nuestro equipo vio a través de un dato que le dieron (no sé si era una IP y demás), y consiguieron determinar dónde se encontraba el objetivo, conseguimos ver quién era, Lo hemos seguido durante quince o veinte días esperando a que llegara la comisión rogatoria internacional que Holanda hizo, y por medio de la cual, a través de los canales de Europol y de Eurojust y la Fiscalía, en este caso de Barcelona, se llevó a efecto la entrada y registro en el domicilio de esta persona y la

intervención de los equipos, con la colaboración de dos policías holandeses que acudieron precisamente aquí para echarnos una mano.

Quiero significar esto, ¿por qué? Porque aquí en España no existía el delito, no teníamos ningún delito sobre este caso, pero teníamos al delincuente. Y en este caso, si no hubiese sido por la actuación nuestra, difícilmente podría haberse llegado a determinar quién era. Quizás en España no ha tenido esa repercusión o esa importancia, pero para esos otros países de la Unión Europea la tuvo, y mucho, por el problema tan importante que generó en la red.

Es un poco el sistema... no sé si es desinteresado, o no es desinteresado; al final Holanda, Alemania y el resto de países y de policías integrantes del contexto de Europol, no solo nos los han agradecido, sino que efectivamente es una forma de confianza de intervenir en muchas más operaciones y en las que seguro que nos hemos ganado su confianza y su participación en otras.

No quiero seguir algunas de las operaciones que se hicieron ya un poco anteriores, sobre Anonymous, operación “Latina”, operación “Escondido”, en fin, no voy a comentar más.

Intervenimos también, por supuesto, en delitos contra la propiedad intelectual e industrial, dentro de las particularidades que tiene, en medicamentos y anabolizantes, en fin.

Esto sí quiero comentarlo al menos brevemente: hay un grupo de actividad que estamos intentando potenciar y es el de redes abiertas. No solamente nos dedicamos a recibir la denuncia o el delito, sino que exploramos en la red para conocer no solamente los delitos que se están produciendo sino determinados comportamientos que socialmente pueden llegar a ser constitutivos de delito. Hablo de cuestiones, por ejemplo, hace año y medio o dos años se tuvo una intervención en la que se producían carreras ilegales de vehículos en Palma de Mallorca con importantes problemas no solamente de

seguridad del tráfico, sino también para las personas, y se consiguió localizar e identificar precisamente a través de Internet.

Cuestiones de identificar ventas de tráficos de armas, anabolizantes, medicamentos falsos, en fin, cuestiones de racismo, xenofobia... Se van tocando determinados problemas sensibles y determinados comportamientos que pueden alterar la vida social.

Y por último, y ya no les canso más, tengo que mencionarle que todo esto no se puede llevar a cabo sin un buen equipo de un área técnica de laboratorio: es imprescindible. A esta gente que tenemos allí yo la llamo "la gente de cacharreo": son los que se encargan de recoger toda la información de los discos duros, los clonados, etc., y hacerlo con las mejores garantías para ponerlo a disposición de la autoridad judicial, y eso implica una labor muy importante de "cacharrear" en esos discos duros, en esos ordenadores, en esos móviles, recoger toda esa información.

Además son los que están más al tanto de cualquier innovación y por eso les tenemos encargado también que participen como profesores en la formación del resto de la gente, en cualquier novedad que aparece, para que de forma integral lo conozca toda la Brigada o toda la Unidad. Y participan tanto en el extranjero como a nivel nacional en cualquier ámbito.

No quiero seguir más. Hay seguramente alguna pregunta de la que han hecho ustedes anteriormente que puede que se haya quedado sin contestar. Si me la repiten, dentro de lo que pueda se la contesto.

Precisamente he visto la primera de ellas, sobre el tema del juego *online*: Precisamente es uno de los temas que estamos explorando en este último grupo que hemos visto de redes abiertas, y realmente resulta inquietante. ¿Por qué? Porque en esta secuencia que les he manifestado antes del desarrollo de la operación "Ransomware", esa parte de organización patrimonial estaba derivando la importante carga de actividad de blanqueo de dinero a través de

diferentes medios, como he dicho antes, y no solamente a través de eso sino a través de juegos *online*. ¿Cómo? Pues lógicamente, a través de dinero virtual que introducen... De todo esto, lo van pasando y van perdiendo pequeños tantos por ciento de comisión, pero esto es algo que tienen de forma estudiada y preparada; saben que de aquí a aquí les va a suponer un 3%, pasa a un 4%, después cogen una "mula" para que lo pase a efectivo, lo meta en otro sitio, de ahí lo pasan... En fin, y ese recorrido lo pueden ir complicando cada vez más para tener cada vez más medidas de seguridad, o según el grado de confianza que tengan en ese grupo en que, como ha dicho el director, tiene externalizado ese servicio la criminalidad. Es verdad que es un tema preocupante el juego *online* y estamos trabajando, estamos explorándolo.

La percepción que tenemos es que a día de hoy estamos viendo todo desde el punto de vista a nivel físico y no sabemos trasladarnos a ese punto de vista virtual en el que los conceptos son distintos y las formas de trabajar son distintas. E intuimos que no solamente la actividad delictiva o el resultado del delito se blanquea por este medio, sino que otras formas de blanqueo de dinero puedan estar pasando por ahí y no lo sabemos.