**COMPARECENCIA DEL DIRECTOR GENERAL DE LA POLICÍA, D. IGNACIO COSIDÓ GUTIÉRREZ, 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 **DIRECTOR GENERAL DE LA POLICÍA** (D. Ignacio Cosidó Gutiérrez): Muchas gracias, presidente. Antes que nada, quiero agradecer a todos los miembros de la ponencia la oportunidad que dan al Cuerpo Nacional de Policía para explicar cuáles son nuestros proyectos, cuáles son nuestras actuaciones, también cuáles son nuestras propuestas en una materia que creo que es importante, y además constituye una de las prioridades, como verán, en nuestra política de seguridad.

Quisiera expresarles además la felicitación, tanto a la Comisión de Interior como a la de Educación y Deporte y a la de Industria, Energía y Turismo, por haber puesto en marcha esta iniciativa, que a mí me parece tan oportuna y tan necesaria.

Por último, también quería decirles que no solo ya como director de la Policía, sino como exsenador, pues es para mí una especial satisfacción volver a esta casa y poner de manifiesto que con iniciativas como esta yo creo que el Senado tiene una importante capacidad para contribuir a hacer una sociedad mejor, que en el fondo creo que es lo que nos anima a todos desde nuestras diferentes perspectivas o ideologías.

Querría pedirles disculpas porque ha surgido un compromiso ineludible con posterioridad a haber acordado ya la fecha y la hora de mi intervención, y yo necesariamente tendré que ausentarme a las once y media, pero también les digo que dado que tanto el comisario jefe de la Brigada de Investigación Tecnológica como la responsable de Redes Sociales dentro del Cuerpo Nacional de Policía

van a intervenir a continuación, pues creo que va a haber oportunidades para que cualquier cuestión que pueda surgir también pueda ser resuelta por ellos.

Es un hecho que las redes sociales se han convertido en parte de nuestra vida, y yo diría que con especial intensidad en la vida de nuestros adolescentes, que a través de esta forma de comunicación los jóvenes se relacionan entre sí, intercambian experiencias, sus gustos, motivaciones y que, en definitiva, las redes sociales son un espacio en el que los jóvenes vuelcan ya gran parte de sus vidas.

Y todo esto en mi opinión tiene efectos muy positivos. Yo creo que toda idea de criminalizar o de tener una visión negativa de todo este fenómeno no es acertada.

Las redes sociales abren formas de comunicación hasta ahora desconocidas, eliminan barreras temporales y geográficas y suponen nuevas oportunidades de comunicación humana. Pero simplemente tenemos que ser conscientes de que también tienen riesgos, como lo tiene conducir un vehículo. Cuando ofrecemos información personal, estamos atentando a veces, y lo que es más peligroso, de forma inconsciente, a nuestra propia intimidad. Porque cada vez estamos más dispuestos a que los demás accedan a determinados aspectos de nuestra vida privada en un afán por mantenernos permanentemente comunicados.

Debemos reconocer que la privacidad en Internet y cómo gestionarla correctamente sigue siendo una asignatura pendiente en nuestra sociedad, y por eso creo en el acierto de esta ponencia.

Los ciudadanos tienen el derecho a decidir quién puede o no utilizar nuestra información, porque lo contrario nos lleva a perder este derecho, de forma que todo lo que colguemos en Internet queda ahí para siempre y al alcance de cualquiera que pueda acceder a ello sin nuestra autorización.

Por desgracia, esta información personal puede ser utilizada por terceros como una forma de acoso, cuando no como un medio para el chantaje o un instrumento para cometer delitos. Estamos hablando en definitiva del cibercrimen como manifestación de los nuevos delitos cometidos mediante la utilización de las tecnologías de la información, contra el cual lucha el Cuerpo Nacional de Policía.

Para comprender la relación que existe entre el cibercrimen y las redes sociales resulta imprescindible contar con una visión panorámica que sitúe cuál es el escenario de nuestra sociedad y cuál es el impacto de estas tecnologías en nuestra sociedad. Yo estoy seguro de que voy a repetir datos y de que probablemente ustedes conozcan mejor que yo esta realidad, pero permítanme recordar de manera muy breve que actualmente uno de cada tres habitantes del mundo es usuario de Internet, es decir, más de 2.400 millones de personas interconectadas cada día entre sí, desde un extremo a otro del planeta, esperando que en el año 2015 sean 2 de cada 3 los ciudadanos del mundo conectados a Internet; que el número de usuarios de telefonía móvil en el mundo alcanza ya el 85,7 % de la población, con 5.200 millones de terminales en uso. Y que dadas las cifras de crecimiento constante de la telefonía móvil, se estima que a lo largo del presente año se alcance el momento en el que por primera vez en la historia una tecnología de consumo igualará en tamaño a la población humana. El número de usuarios de las redes sociales supera además los 3.000 millones de usuarios; tengan presente que una persona en muchas ocasiones tiene más de una vinculación a una red social, pero son 3.000 millones de usuarios.

Nuestro país se incorporó hace ya años al tren de las tecnologías de la información, y creo que es importante cuando hablamos de estas cuestiones, no hablar de futuro, sino decir que esta es una realidad que está presente y que está plenamente consolidada. En 2012 existían en España más de 24 millones de internautas, lo que significa casi un 70% de la población española, y el 73% de

esos internautas accede a Internet diariamente. Y el porcentaje llega al 85% si nos referimos a los jóvenes, entre 16 y 24 años.

¿Cuál ha sido el gran motor de crecimiento? La telefonía móvil, que es utilizada casi ya por la mitad de los internautas para acceder a Internet. De hecho, el 63% de los usuarios de móvil en España utiliza un *smartphone*, lo que representa el porcentaje más alto entre las cinco mayores economías de la Unión Europea.

De acuerdo con el primer estudio sobre redes sociales en España del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, que no sé si habrá ya comparecido, España ocupa el tercer puesto en el ranquin mundial de usuarios activos en las redes sociales, con un 77% de los usuarios de Internet. Y uno de cada tres de estos usuarios de las redes sociales se conecta todos o casi todos los días. Y el 41% de ellos de 19 a 25 años utiliza dos redes sociales de media.

Yo insisto, creo que todo esto es sumamente positivo, es decir, creo que esto es bueno. Sin embargo, y como muy acertadamente señala la propia constitución de esta comisión por el Pleno del Senado, en la creación de la presente ponencia, existen otros datos que sí resultan preocupantes: el 75% del total de los entrevistados por el Observatorio se muestra poco o nada preocupado acerca de lo que otras personas vean o piensen de ellos a través de las redes sociales. Y yo les diría que aquí el reto fundamental son los menores. Los menores acceden a páginas de temáticas y contenidos inadecuados, ya estemos hablando de pornografía, de violencia, sexismo, racismo, apología de la drogadicción, a veces apología del suicidio o de enfermedades como la anorexia. Pueden sufrir un potencial encuentro físico con sujetos que enmascaran su identidad en la red para invitar a los niños a diferentes chats o luego tratar de citarse personalmente con ellos. Pueden sufrir fraudes en ventas de artículos, incluso pueden ser objeto de espionaje, en el sentido de tratar de captar

información personal o de su entorno familiar, ya que los menores son especialmente proclives a facilitar ese tipo de información.

Los profesionales de la seguridad saben que tienen un reto formidable para garantizar la seguridad de todos los usuarios en la red, pero yo diría que de manera muy particular en el caso de los menores.

Este problema ha crecido además de forma paulatina hasta alcanzar unas cotas que ciertamente resultan preocupantes. De tal suerte que actualmente el delito más lucrativo a nivel mundial después de la prostitución y el tráfico de drogas es el cibercrimen. Internet se ha convertido en una infraestructura de información tan esencial para las personas que es imprescindible que nuestras redes y sistemas informáticos sean resistentes, confiables y seguros ante todo tipo de amenazas. Y en este sentido la seguridad se configura como un presupuesto necesario para el efectivo desarrollo de la sociedad de la información.

En Internet el clásico debate entre libertad y seguridad se concilia cuando se trata del ejercicio de derechos y libertades en Internet: una red abierta y libre, necesariamente tiene que ser una red segura. En la Agenda Digital para Europa que ha elaborado la Comisión Europea se reconoce que los ciudadanos no emprenderán actividades en línea cada vez más sofisticadas si no están convencidos de que tanto ellos como sus hijos pueden fiarse plenamente de las tecnologías de la información. Por tanto, la Comisión insta a los Estados miembros a combatir el auge de las nuevas formas de delincuencia, la ciberdelincuencia, que abarca una amplia tipología de delitos, como ya les he señalado, desde la pornografía infantil al robo de identidades o los ciberataques.

La propia Comisión Europea aprobó en 2012 su primera estrategia en favor de un Internet más adecuado para los niños. En esa estrategia señala que los menores en Internet merecen un tratamiento específico para conseguir que la red se convierta en un lugar seguro en el que los niños puedan acceder al

conocimiento, comunicarse, desarrollar sus aptitudes y mejorar sus perspectivas, incluso laborales, de futuro. Pero que los riesgos experimentados por los jóvenes en Internet son bastante evidentes, y similares además en toda Europa.

En 2010, cuatro de cada diez menores en Europa dijeron haber encontrado uno de los siguientes riesgos: comunicación en línea con alguien que no conocían personalmente; exposición a contenidos inapropiados para su edad generados por usuarios en los que se promovía la anorexia, la automutilación, el consumo de drogas o el suicidio; exposición a imágenes sexuales en línea y uso indebido de los datos personales; encuentros en el mundo real con personas conocidas en línea; o ser víctimas de ciberacoso. Es decir, esto, cuatro de cada diez menores entrevistados.

Surgen además nuevas pautas de comportamiento, como la distribución de imágenes de agresiones físicas a otros niños tomadas con la cámara de un móvil, o el envío a compañeros de imágenes o mensajes con contenido sexual.

Además se está expandiendo el uso de Internet para la captación de víctimas, para la trata de personas y la publicidad de sus servicios, incluyendo en ocasiones a los menores.

Conocen además que Internet constituye un vehículo para la fácil difusión de la pornografía infantil. Lamentablemente hoy daremos cuenta de una nueva operación en relación con esta cuestión. Son numerosos los retos que debemos encarar los responsables públicos para luchar contra el cibercrimen, y en espacial contra el que afecta a jóvenes y menores.

Permítanme comentarles muy brevemente tres características de Internet que hacen especialmente difícil el trabajo de persecución del delito en la red, que llevan a cabo profesionales como el comisario que a continuación les va a hablar.

En primer lugar, Internet es muy complejo, es un sistema, yo diría casi un ecosistema tecnológico en el que intervienen entidades públicas y privadas con

intereses muy diversos y que en ocasiones resultan contradictorios. Para garantizar la seguridad de nuestros jóvenes en Internet entran en juego desde la responsabilidad primera de los padres, los centros educativos, la industria de los contenidos digitales, los operadores de telecomunicaciones, los proveedores de acceso a Internet, los fabricantes de equipos y de software, las asociaciones en defensa de los derechos de los menores, y lógicamente los poderes públicos; el poder legislativo, muy en primera instancia, pero los organismos reguladores, los jueces y tribunales y, por supuesto, las Fuerzas y Cuerpos de Seguridad del Estado. Son muchos actores.

En segundo lugar, en Internet, como bien conocen, no hay fronteras ni físicas ni geográficas. En el cibercrimen es muy habitual que la víctima y el autor del delito estén separados por miles de kilómetros en países diferentes. El carácter de amenaza global del crimen organizado se ve potenciado por el empleo y el aprovechamiento de estas nuevas tecnologías que permiten a las redes criminales actuar desde lugares donde pueden sentirse seguros frente a la acción penal y procesal, canalizando sus beneficios ilícitos mediante un sistema financiero global. Esto supone un importante reto de cooperación policial internacional, al tener que coordinar actuaciones policiales de varios países, y además a mucha velocidad para poder ser eficaces en la lucha en este delito.

Y en este campo, quiero decirles que estamos avanzando de manera muy notable. Un ejemplo es la reciente detención en Dubái en febrero de este año de un ciudadano ruso autor del conocido “virus de la policía”, quien utilizaba una célula financiera radicada en la Costa del Sol en una operación que fue protagonizada por la Brigada de Investigación Tecnológica. Y otro éxito muy reciente es la detención en Barcelona el pasado mes de abril de un activista holandés responsable del mayor ataque de denegación de servicio distribuido de la historia, quien en marzo de 2007 colapsó el funcionamiento de Internet en

todo el mundo. Por tanto, segunda característica: el carácter global que tiene este fenómeno.

La tercera característica que hace especialmente difícil la lucha contra el cibercrimen es la especialización y organización del mismo. Dejando aparte los casos de acosos entre menores que se producen en entornos escolares, puede decirse que lamentablemente el cibercrimen en general se ha convertido en un negocio que mueve un elevadísimo volumen de dinero. De acuerdo con el *Internet Crime Complaint Center*, que es un centro respaldado por el FBI, las pérdidas totales en el año 2009 debidas a cibercrimen ascendieron a 500.000 millones de dólares en el mundo. Un informe de 2011 de la empresa Norton señaló que el coste del cibercrimen se acerca al valor del tráfico de drogas, es decir, al valor global del tráfico de droga, y si lo quieren tomar como referencia, el cibercrimen supera en más de cien veces los gastos anuales de Unicef.

Por su parte, Europol ha puesto en evidencia que el modelo de negocio cibercriminal difiere significativamente de la tradicional delincuencia organizada, porque el ciberespacio y la infraestructura de Internet contribuyen a hacer del cibercrimen un modelo orientado al servicio, donde no hay jerarquía, sino proveedores de servicios cibercriminales unificados por la propia infraestructura del ciberespacio. Es lo que podemos denominar como “el crimen como servicio”.

La consecuencia es que las plataformas tecnológicas que utilizan los cibercriminales son multicrimen. Pongo un ejemplo: una red de miles de ordenadores infectados, lo que se denomina una *botnet*, puede ser ofertada por una organización criminal para distribuir correos electrónicos fraudulentos (la práctica conocida como *phishing*) o para la realización de un ataque de denegación de servicio a otras organizaciones criminales. Las redes Tor permiten intercambiar de forma anónima todo tipo de contenido delictivo, desde material de pornografía infantil hasta mensajes entre terroristas. Otro ejemplo:

Internet ofrece medios cada vez más perfeccionados para poder blanquear los beneficios financieros obtenidos del cibercrimen de forma ilícita por las empresas de cibercriminales.

Por lo tanto, si bien el Código Penal tipifica de forma separada los distintos tipos de delito, desde la Policía Nacional creemos que es imprescindible una estrategia transversal de lucha contra el cibercrimen, precisamente por esta naturaleza que tiene de criminalidad como servicio. No se puede resolver un problema concreto de abuso sexual de menores sin tener una estrategia integral para la lucha general contra el cibercrimen.

Los delitos cibernéticos a los que nos enfrentamos son de muy variado tipo. En el Convenio sobre la Ciberdelincuencia del Consejo de Europa, firmado en Budapest en el año 2001, se utiliza el criterio de diferenciar dos tipos básicos: el que tiene como objetivo el sistema de información, o bien el que utiliza estas tecnologías como forma para cometer otros delitos que tradicionalmente ya se cometían.

Así, siguiendo esta clasificación, se encuentran los delitos en los que el ordenador, la red informática o un dispositivo electrónico es el objetivo propio de la actividad criminal. Los delitos contra los que lucha la Policía Nacional en este primer campo son, entre otros, los accesos no autorizados a sistemas de información, como por ejemplo la piratería o *hacking*, para copiar, modificar, borrar o destruir datos y programas; la difusión de códigos maliciosos, el *malware*, tales como los virus, los gusanos, los troyanos o las bombas software; la interrupción o denegación de los servicios, por ejemplo, los ataques de denegación de servicios DoS, el robo o mal uso de los servicios, como puede ser el robo de una cuenta en Internet o de un nombre de dominio, para después enviar con identidad falsa mensajes; o finalmente, los ataques contra infraestructuras críticas fundamentales, con consecuencias potencialmente

desastrosas para el conjunto de la sociedad, lo que podríamos denominar como ciberterrorismo.

Para clarificar este tipo de delitos, les citaré brevemente dos casos de éxito de operaciones importantes de la Policía Nacional. El primero de los casos fue la reciente detención de un pedófilo *hacker* que grababa imágenes de la vida íntima y sexual de sus vecinos a través de las cámaras web de los ordenadores personales de estos. El sujeto asaltaba las conexiones WiFi de sus vecinos, les infectaba los ordenadores con un *malware* tipo troyano que le permitía controlarlos a distancia y grabar a los propietarios con las cámaras de sus propios ordenadores infectados.

El segundo caso consiste en la detención el pasado mes de 35 personas de una red internacional especializada en la clonación de tarjetas bancarias. La red criminal operaba a nivel mundial e instalaba dispositivos para clonar las tarjetas (lo que conocemos como *skimming*) en cajeros automáticos y datáfonos. Copiaban los datos de las tarjetas y se los enviaban a otros integrantes de la banda para su falsificación y uso. Y finalmente enviaban el dinero fuera de España para blanquearlo.

Igualmente la Policía Nacional lucha de forma eficaz contra las redes de pederastia y pornografía infantil. Los éxitos más recientes de operaciones policiales son la detención en Barcelona en noviembre de 2012 del pederasta que acosó a 50 menores a través de videoconsolas, la detención en Gandía en abril de este año del acosador sexual de 300 niñas a través de Internet, y también este mismo mes la detención de 25 personas y la imputación de otras 16 por pornografía infantil dentro de la denominada operación “Ciudadano”. Esta operación, la operación “Ciudadano”, es un buen ejemplo de colaboración ciudadana, ya que se realizó gracias a las informaciones aportadas por los ciudadanos a través de denuncias realizadas en las comisarías de policía y

también las remitidas al correo electrónico de la policía, correo que había sido difundido a través de los canales de redes sociales de la Policía Nacional.

Yo destacaría –luego lo haré– que aquí es básico y fundamental la colaboración ciudadana. Sin eso es muy difícil que nosotros podamos ser eficaces.

Los tres principales problemas a los que se enfrentan nuestros jóvenes y menores son: en primer lugar, el acceso a contenidos inapropiados, como les mencionaba y les enumeraba antes.

En segundo lugar, cada vez más casos de acoso en línea (lo que se denomina como el ciberacoso o el *ciberbullying*). Este tipo de ciberdelincuencia implica el uso del ordenador para causar un daño personal al menor, por ejemplo ansiedad, angustia o daño psicológico. Y lamentablemente hemos llegado a tener casos de suicidios como consecuencia de este tipo de acoso. Se considera como tal el envío de *e-mails* abusivos, amenazantes o de odio, la publicación de información lesiva para una persona en páginas web, foros o redes sociales, bien a través del ordenador, de las tabletas, de los teléfonos móviles, con la intención de intimidar, amenazar o acosar a la víctima, normalmente con intención de dañar su imagen.

Y el tercer gran problema que se encuentran los menores es el abuso sexual infantil (también denominado el *child grooming*). Este ciberdelito abarca una serie de conductas que tienen un elemento objetivo de daño sexual al menor, como son las acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con el objetivo de obtener imágenes eróticas o pornográficas del mismo para satisfacción sexual o incluso como preparación o chantaje para un posterior encuentro.

Según las normas internacionales, esta conducta incluye la producción, la posesión y el acceso a imágenes que registren el abuso sexual de niños por parte de adultos, así como de imágenes de niños involucrados en una conducta

sexualmente explícita o de los órganos sexuales. Este tipo de imágenes son producidas y utilizadas principalmente para fines sexuales con o sin el conocimiento del niño.

Desde una perspectiva práctica, este tipo de ciberdelincuencia se puede clasificar en tres componentes: la producción, que es la creación del material; la distribución, la carga y difusión del material; y el consumo, la descarga del material.

Desgraciadamente la capacidad para obtener y almacenar imágenes y contenidos se ha facilitado por la ubicación de las redes de comunicación y por los avances relacionados con la tecnología digital, es decir, cualquiera puede grabar con un teléfono móvil o con cualquier dispositivo a muy bajo coste, y además almacenarlo en dispositivos con una enorme capacidad.

El *child grooming* es un proceso que comúnmente puede durar semanas o incluso meses. Comienza cuando el adulto procede a entablar lazos de amistad con el menor, normalmente simulando ser otro menor. De esta forma, el adulto va obteniendo datos personales y de contacto. En un segundo momento, y utilizando tácticas como la seducción o la provocación, por ejemplo mediante el envío de imágenes en bañador o ropa interior, el delincuente consigue finalmente que el menor se desnude frente a la *webcam* o le envíe fotografías de naturaleza sexual. A partir de ese momento el menor está perdido, ya que el pederasta inicia un ciberacoso de chantaje a la víctima para obtener cada vez más material pornográfico en una espiral creciente de mentiras y miedos dirigidos a tener un encuentro físico con el menor para abusar sexualmente de él.

Puedo asegurarles que la Policía Nacional tiene la más firme determinación para luchar contra todas las formas que pueda adoptar el cibercrimen en general, pero yo les diría que de forma especial contra estas formas de cibercriminalidad a las que nos estamos refiriendo. Como muestra de este compromiso hemos decidido potenciar la unidad responsable de la lucha

contra este tipo de delitos mediante la creación de una nueva unidad de investigación tecnológica encuadrada dentro de la Comisaría General de Policía Judicial. La idea es transformar la actual brigada en una unidad de la que dependan dos brigadas: una Brigada Central de Investigación Tecnológica, a la que corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial, y los fraudes en las telecomunicaciones; y una segunda brigada, que sería la Brigada Central de Seguridad Informática, a la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica, es decir, a la seguridad de los sistemas, y a los fraudes.

El responsable de esta unidad intervendrá posteriormente para exponer a sus señorías cómo se realiza el trabajo de investigación y de persecución de estas actividades delictivas. Pero la creación de esta unidad, yo querría destacar que pretende duplicar el número de efectivos dedicados a la lucha contra el cibercrimen y dotarles además de los medios tecnológicamente más punteros y especializados para que cumplan eficazmente su función de dar confianza a nuestros ciudadanos en el ciberespacio.

Yo les diría que ninguna tipología delictiva está creciendo al ritmo al que lo está haciendo la ciberdelincuencia, y que, por tanto, es imprescindible que aumentemos nuestras capacidades para poder investigar este tipo de delitos.

Pero no se trata solo de crear una nueva unidad para luchar contra el cibercrimen, porque yo creo que lo más importante es conseguir que la totalidad de las unidades de la Policía Nacional, por supuesto las unidades territoriales de Policía Judicial, pero de manera especial las unidades centrales especializadas asuman una parte de la responsabilidad en la lucha contra esta ciberdelincuencia.

Así, la Comisaría General de Información debe realizar una especial vigilancia digital de la red en su lucha contra el terrorismo y el “hacktivismo”. La Comisaría General de Seguridad Ciudadana realiza el seguimiento en redes

sociales y foros de aquellos perfiles de grupos violentos que puedan derivar en violencia en nuestras calles. La Comisaría General de Policía Científica está trabajando en informática forense y en la captura y preservación de evidencias digitales. La Unidad de Informática es responsable de dotar de las herramientas y el apoyo tecnológico a todas estas unidades. La Unidad de Cooperación Internacional debe establecer mecanismos de interrelación más eficaces para luchar contra este tipo de delincuencia.

Pero si tuviera que destacar, más allá de la propia unidad de investigación, unas unidades que resultan fundamental en esta estrategia son aquellas que se dedican a la colaboración ciudadana. Porque todas las actuaciones de difusión y prevención que realizamos en este ámbito, creo que son trascendentes si realmente queremos tener eficacia en la lucha contra este fenómeno. Y en ese sentido la inspectora que es responsable de redes sociales dentro del Cuerpo Nacional de Policía les informará con más detalle de cuáles son esas iniciativas.

Con esta visión integral del cibercrimen, la Policía ha aprobado un Plan estratégico que abarca los años 2013 a 2016. En este plan se recogen los objetivos prioritarios para la Policía Nacional en los próximos años, y pone en marcha un plan de transformación de la Policía que está basado en muy buena medida en la innovación tecnológica y en un uso más eficiente de los recursos para lograr que España sea un país más seguro. El plan pretende la transformación del Cuerpo Nacional de Policía en una verdadera "Policía Inteligente" a través de un objetivo que hemos denominado "Policía 3.0".

¿Cuáles son las prioridades de este plan?

Claramente hemos situado el ciberdelito como una de las prioridades máximas, como uno de los objetivos estratégicos del Cuerpo Nacional de Policía. La estrategia a seguir en los próximos cuatro años y sus objetivos han sido establecidos con especial compromiso en la transparencia y en la participación ciudadana. Se va a potenciar la colaboración ciudadana a través de

las redes sociales y el contacto constante con sus unidades de participación ciudadana.

Como medidas concretas que se recogen en este plan se encuentran la de impulsar las investigaciones relacionadas con los fenómenos delictivos emergentes derivados del uso de las tecnologías de la información; realizar la respuesta ante la proliferación de los delitos contra las personas cometidos a través de la red, especialmente en el ámbito de la protección al menor y la explotación sexual infantil; potenciar las investigaciones relacionadas con amenazas y vulnerabilidades a los sistemas informáticos, así como la actividad delictiva derivada de las mismas, con especial incidencia en la protección de las infraestructuras críticas; promover y participar en las investigaciones de investigación y desarrollo y colaborar con otras instituciones públicas y privadas, e impulsar el desarrollo y actualización de herramientas técnicas legales para una mejor eficacia contra este tipo de delincuencia; así como participar en instituciones internacionales (yo destacaría en este campo Interpol y Europol, y de manera muy particular un centro de nueva creación, el *European Cybercrime Center*, creado en el seno de Europol), así como incrementar la cooperación bilateral que mantenemos con otras policías en este tipo de delincuencia. Les puedo decir que la Policía Nacional está formando policías de otros países del norte de África o de Iberoamérica en relación con las técnicas de investigación de este tipo de delincuencia.

Una medida de gran relevancia para luchar contra este ciberdelito es la creación en el seno del Cuerpo Nacional de Policía de un equipo de respuesta a emergencias informáticas. Una tarea fundamental de este CERT de la Policía Nacional será la coordinación centralizada para las cuestiones relacionadas con seguridad de las tecnologías de la información dentro del Cuerpo Nacional de Policía. Desde una perspectiva externa, el CERT debe mantener una relación fluida y constante con otras fuerzas y cuerpos de seguridad del Estado, con otros

CERT públicos y privados y con entidades europeas, no solamente Europol, sino también ENISA.

Junto a todas estas medidas, reviste especial importancia la consideración que da el plan estratégico a la formación del personal del Cuerpo Nacional de Policía en materia de ciberseguridad. Y en este campo pretendemos aumentar la formación en ciberseguridad en los planes de estudio del personal de nuevo ingreso, para dar ya una información básica en nuestras escuelas de policía, y diseñar e impartir una formación especializada, específica, para las unidades del Cuerpo Nacional de Policía que trabajan en este campo. Y esa formación, necesariamente tiene que ser una formación en colaboración con entidades externas, con otros CERT, con la universidad, con entidades privadas, incluso con empresas, porque este es un mundo que evoluciona a tal velocidad que uno no puede nunca aspirar a ser autosuficiente.

Otra medida importante incluida en el Plan Estratégico es la revisión –y esto les afecta de manera muy directa– del actual marco normativo y de colaboración en materia de ciberseguridad. En este sentido, considero que es necesaria una reflexión sobre la legislación existente para eliminar posibles barreras a una actuación policial eficaz, teniendo presente siempre la salvaguarda de los derechos fundamentales, del derecho a la intimidad de todos los ciudadanos. Y por eso es importante no solamente hacer esta reflexión sobre la legislación, sino establecer protocolos muy precisos para el intercambio de información con los operadores de telecomunicaciones y los proveedores de acceso a Internet, siempre con un escrupuloso respeto al marco legal de protección de datos de carácter personal, que les puedo asegurar que en España es particularmente exigente. Esta ponencia, estoy seguro de que va a hacer alguna aportación importante en ese terreno.

Para mejorar los niveles de seguridad ciudadana, el plan estratégico diseña un nuevo sistema –si me permiten– de patrullaje inteligente, e implementa una

nueva herramienta informática para la gestión de los servicios de protección a nivel nacional.

Por otra parte, la preocupación de los grupos vulnerables se convierte en otro objetivo prioritario de la Policía, por lo que impulsaremos una actuación policial integral que consiga un aumento de la prevención, la efectiva protección de las víctimas y una mayor eficacia en la investigación de los hechos delictivos.

Con el objetivo de promover la seguridad de los menores, muy particularmente en el entorno escolar y las redes sociales, se va a intensificar la participación en los programas de concienciación para un uso seguro y responsable de las redes sociales; se fomentará la colaboración entre las administraciones y con los administradores de estas redes en la protección del menor; y se intensificarán y mejorarán las campañas de educación en seguridad en el entorno escolar, con especial atención al acoso escolar y al *sexting*, y se promoverán campañas que prevengan su integración en actividades delictivas, así como su captación por bandas juveniles.

Y finalmente –y termino ya– el Plan Estratégico realiza también una apuesta decidida por la participación ciudadana, no como una necesidad impuesta desde el exterior, sino como un valor que debe formar parte cada vez más de nuestra propia cultura policial. El nuevo marco de seguridad pública exige abrirse a la colaboración ciudadana facilitando su participación e integración, habilitando nuevos canales de comunicación a través de las redes sociales. No voy a hacer publicidad porque ya lo conocen todos ustedes, pero creo que la Policía Nacional es en estos momentos una clara referencia internacional para otros cuerpos de seguridad de cómo utilizar las redes sociales para mantener una comunicación y para mantener una colaboración con los ciudadanos.

Señorías, como resumen de mi intervención, puedo decirles que el Cuerpo Nacional de Policía se encuentra comprometido en la lucha contra el

cibercrimen, y en especial en la lucha contra todas las manifestaciones de delitos que afectan a nuestros menores en su relación con las tecnologías de la información, que creo que en este campo es el principal reto que tenemos común.

Un marco adecuado de seguridad es el presupuesto necesario para construir una sociedad de la información libre. En este empeño –como ven– estamos trabajando con mucho entusiasmo, y quiero reiterarles toda nuestra colaboración para el éxito de esta ponencia, que estoy seguro de que va a contribuir también de manera decisiva a este reto común que tenemos por delante.

Muchísimas gracias, y siento haberme extendido más de lo que inicialmente el presidente me había sugerido, aunque en este trámite parlamentario entiendo que no había esta limitación temporal. Escucho con toda atención sus intervenciones, y si queda alguna cuestión más por contestar, seguro que los otros representantes del Cuerpo Nacional de Policía pueden también participar en el mismo.