DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 118 | Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DEL EXCMO. SR. D. JOSÉ MANUEL GARCÍA-MARGALLO Y MARFIL

Sesión núm. 22

celebrada el jueves 8 de noviembre 2018 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

---

cve: DSCG-12-CM-118

Se abre la sesión a las doce y cuarenta y cinco minutos del mediodía.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Buenos días, señorías. Damos comienzo a la sesión de la Comisión Mixta de Seguridad Nacional, que tiene el siguiente orden del día: Comparecencia de don Rafael Pérez Pérez, comisario principal de Policía Nacional y director de la Unidad Central de Ciberdelincuencia, encuadrada en la Comisaría General de la Policía Judicial, para informar sobre diversas cuestiones relativas a la ciberseguridad en España.

Iniciamos la sesión dándole la bienvenida y agradeciéndole su comparecencia ante esta Comisión. Tiene usted la palabra para intervenir por el tiempo que estime oportuno y después pasaríamos al turno de los grupos parlamentario. Muchas gracias y bienvenido.

El señor **COMISARIO PRINCIPAL DE LA POLICÍA NACIONAL Y DIRECTOR DE LA UNIDAD CENTRAL DE CIBERSEGURIDAD** (Pérez Pérez): Muchas gracias. Buenos días a todos.

Con permiso, señor presidente, señoras y señores diputados y senadores, es un honor, un placer y desde luego una responsabilidad representar al Cuerpo Nacional de Policía en esta Comisión Mixta y voy a tratar de explicarles en los próximos minutos qué hacemos desde la Policía Nacional en la lucha contra la ciberseguridad y la ciberdelincuencia, esencialmente en la ciberdelincuencia. Me gustaría situar mi exposición al hilo de las funciones que ejerzo como jefe de la Unidad Central de Ciberdelincuencia. Como saben ustedes, la Unidad Central de Ciberdelincuencia está incardinada dentro de la Comisaría General de Policía Judicial. En consecuencia, en mi intervención no voy a hablar ni de ciberterrorismo, que corresponde en exclusiva en la Policía Nacional a la Comisaría General de Información, ni voy a hablar tampoco de infraestructuras críticas, habida cuenta que entiendo que el órgano técnico del Ministerio del Interior es la Oficina de Coordinación Cibernética.

Mi exposición la he estructurado en cuatro bloques fundamentales. En el primero de ellos les haré una aproximación muy breve de lo que representa el uso de las tecnologías y qué incidencia estamos teniendo en el uso de las mismas, con una referencia a nuestro origen allá por el año 1995. El segundo bloque lo centraré y sustentaré esencialmente en el informe que anualmente elabora la Secretaría de Estado de Seguridad, el informe sobre cibercriminalidad en España del año 2017, con los datos que se incorporan en el sistema estadístico de criminalidad y, sobre la base de esa situación de la ciberdelincuencia, quiero comentarles qué respuesta estamos dando desde la Dirección General de la Policía, desde la Policía Nacional, a través esencialmente de nuestro Plan estratégico institucional y con el apoyo y la estructura, tanto central como periférica, que tenemos en esta unidad de ciberdelincuencia. Finalmente, concluiré con unas líneas de mejora que, desde mi punto de vista, podrían conseguir una mayor concienciación de los ciudadanos a la hora de abordar estos fenómenos de ciberdelincuentes.

Comenzaré haciendo esa referencia muy breve a nuestros orígenes. Nosotros nacimos en el año 1995 y aquel grupo encuadrado dentro de la Policía Judicial estaba integrado única y exclusivamente por cuatro funcionarios. Indudablemente, aunque se podía percibir, no podíamos imaginar cuál sería la influencia real que iban a tener las nuevas tecnologías, y esencialmente el uso de Internet, en nuestras actividades diarias. Era un grupo que no disponía —como afortunadamente ahora contamos en la unidad— de la capacitación técnica y académica con la que ahora contamos. **(El señor presidente ocupa la Presidencia).** Ahora en la unidad contamos con ingenieros de telecomunicaciones, ingenieros físicos y formación profesional de segundo grado, es decir, con una capacitación académica debidamente acreditada para hacer frente a esta lucha. Sin embargo, en aquellos momentos éramos un grupo de funcionarios con la investigación como oficio y lo fundamentábamos esencialmente en esas relaciones que podíamos mantener con las empresas del sector para preguntarles las dudas que evidentemente nos iban surgiendo. Señalo que no teníamos la capacitación técnica que tenemos ahora e incluso podríamos hablar de hasta qué punto pecábamos de ingenuidad, porque pedíamos directamente a las empresas proveedoras de servicios, mediante un oficio policial, cuál era la titularidad de una IP, cosa para la que ahora, como ustedes sabe, necesitamos una autorización judicial.

Sin duda, volviendo otra vez al presente, Internet nos ha abierto un nuevo camino, nos ha abierto unas posibilidades que realmente antes no teníamos. Ahora desde Internet podemos hacer compras, buscar información que nos interese, podemos hablar con determinadas personas que están en otra parte del mundo, pero indudablemente esos beneficios que conlleva Internet, también conllevan una serie de amenazas y riesgos que incluso ya la propia Estrategia de Ciberseguridad Nacional reconoce. Es decir, ahora lo que se denomina el ciberespacio se ha convertido en el canal o vehículo por donde circulamos todos y debemos proteger —y en esto está la Policía— el ciberespacio. Como les decía, la Estrategia de

cve: DSCG-12-CM-118

Ciberseguridad Nacional habla de que se han eliminado fronteras de distancia y tiempo. Indudablemente desde nuestro ordenador o desde nuestro teléfono móvil podemos conectarnos con cualquier persona en otra parte del mundo.

En la unidad entendemos que los delitos tecnológicos se pueden abordar desde dos puntos de vista: primero, aquellos delitos tecnológicos en los que se utiliza la propia red para causar daño a otros equipos u otros sistemas informáticos: denegaciones de servicio, intrusiones, ataques informáticos y, segundo, delitos tradicionales en los que Internet se constituye como un instrumento para la comisión de dichos delitos: injurias, amenazas, calumnias, delitos de odio, etcétera. No quiero desaprovechar la ocasión para poner de relieve en este foro las limitaciones con las que nos encontramos de manera inicial a la hora de abordar nuestras investigaciones. La primera de ellas es que la ley siempre va por detrás de las tecnologías, aunque indudablemente hemos tenido avances sustanciales. Como ustedes conocen, en el año 2015 se aprobó la Ley de Enjuiciamiento Criminal que nos atribuye muchos más medios de investigación procesal en el tema de la ciberdelincuencia, pero realmente siempre las tecnologías van mucho más por delante que nosotros. La segunda limitación con la que nos encontramos —no sé si ha sido objeto de debate en algún momento en este foro— es el principio de territorialidad de nuestras leyes. Les hablaba de que el ciberespacio actualmente no conoce fronteras. En el ciberespacio actualmente no tenemos delimitado hasta dónde se llega y hasta dónde no se llega e indudablemente necesitamos que ese espacio se haga cada vez mayor. Finalmente, la tercera limitación con la que nos enfrentamos es la disparidad de legislaciones; simplemente a nivel europeo debemos enfrentarnos a diferentes legislaciones, que son las que tenemos. Tenemos una ventana abierta a través de la Convención de Budapest del año 2001, ratificada por España en el año 2010, ya que los dos objetivos fundamentales de la Convención de Budapest son que podamos armonizar nuestras legislaciones y tener un reforzamiento de la cooperación internacional. Para concluir con este primer bloque, les tengo que decir que fueron cuatro los funcionarios que inicialmente crearon el grupo de delitos informáticos cuando nació. Actualmente la Dirección General de la Policía ha reforzado la unidad que dirijo y ha reforzado también los servicios periféricos. Ahora dependen directamente de mí más de un centenar de funcionarios de Policía de todas las escalas y, a nivel de estructura periférica, en todas y cada una de nuestras jefaturas superiores tenemos grupos de delitos tecnológicos y en la mayoría de las comisarías provinciales también tenemos grupos de delitos tecnológicos.

Una vez hecha una aproximación a lo que representa el uso de Internet, me voy a fundamentar en un informe objetivo que realiza la Secretaría de Estado de Seguridad sobre la criminalidad informática y les voy aportar una serie de datos, aunque probablemente ustedes ya los conozcan. Antes de entrar en ellos, quiero hacer una pequeña aproximación a cuál es la radiografía de la sociedad de la información de nuestro país. En el informe consta que más del 78 % de las personas tienen un ordenador de su casa. Por otra parte, la utilización de Internet ha crecido desde el año 2008, en que la utilizaban una media del 60 %, hasta un 84,6 %; es decir, el crecimiento de la utilización de Internet no es exponencial pero sí progresivo. En cuanto al rango de edad —que quizá es lo más significativo—, vemos que el 98 % de los jóvenes comprendidos entre dieciséis y veinticuatro años han utilizado Internet en los últimos tres meses. Sobre esa base, desde mi punto de vista ahora les tengo que explicar cuál ha sido el crecimiento de los ciberdelitos. Hay que reconocer, porque es un hecho objetivo, que entre los delitos conocidos por la secretaría de Estado el año pasado —lo que no quiere decir que sean los únicos que se han cometido— ha habido más de 81 000 infracciones. Por tanto, hemos tenido en 2017 un crecimiento de un 22,1 % con respecto a 2016. De esos más de 81 000 delitos, el 74,4 % corresponden a estafas a través de Internet, situándose en segundo lugar las amenazas y coacciones con un 14 %. Con esto no pretendo alarmarles, sino simplemente darles los datos y, al mismo tiempo, lanzar un mensaje de confianza en la Policía y en las Fuerzas y Cuerpos de Seguridad del Estado; así lo haré a lo largo de toda mi intervención y lo argumentaré con acciones concretas que hemos venido realizando A pesar de ese incremento del 22,1 %, he de decir que nuestra eficacia policial ha mejorado algo más de un 27 % y el número de detenidos el año pasado ha sido de más de 4900 personas.

Ante este panorama, las preguntas que nos podemos hacer todos son qué hace la Policía Nacional ante ese crecimiento, qué respuesta estamos dando y cómo estamos estructurados. La respuesta la tenemos inicialmente en el Plan Estratégico Institucional 2017-2021 de la Dirección General de la Policía, que contiene como premisa fundamental que la lucha contra la ciberdelincuencia es, en primer lugar, un área prioritaria para la Dirección General de la Policía; en segundo lugar, es un área transversal a la comisión de muchos delitos; y, finalmente, es un área que requiere una alta especialización por parte de los integrantes de las unidades que se ocupan de investigar estas tipologías. En ese Plan Estratégico

cve: DSCG-12-CM-118

Institucional tenemos un objetivo primordial, que es prevenir y luchar contra la delincuencia potenciando la ciberseguridad. Asimismo, para dar cumplimiento a este plan estratégico, tenemos tres objetivos específicos —y ahora entraré en cada uno de ellos— que voy a correlacionar con cada una de las estructuras policiales de las que dispone la unidad central y la mayoría de los grupos de delitos tecnológicos de las provincias de la periferia.

El primer objetivo específico que contempla el Plan Estratégico Institucional es detectar las amenazas y vulnerabilidades de los sistemas informáticos. Como es evidente, este objetivo se encamina a la protección del ciberespacio a la que he hecho referencia antes. Nosotros, como Policía judicial, debemos averiguar la comisión de delitos informáticos, perseguir al delincuente y ponerlo a disposición de la autoridad judicial. Por tanto, el objetivo es proporcionar mayor seguridad en el ciberespacio y de eso se ocupa la Brigada Central de Seguridad Informática, que está integrada a su vez por dos secciones operativas: una sección que investiga y desarrolla inteligencia sobre ciberamenazas y una sección de seguridad lógica, que probablemente es la sección más operativa y que realiza las investigaciones consecuencia de los ataques que se vienen produciendo. Indudablemente para investigar los hechos o los ataques, como no se le puede escapar a nadie, debemos en primer lugar conocer qué ataque se ha sufrido, quién ha sufrido ese ataque, qué daños ha ocasionado y a qué aparatos o equipos ha afectado; es decir, todos los datos técnicos que deben ser facilitados por el administrador de la empresa y que se deben poner en nuestro conocimiento. Desgraciadamente eso no es así —he de reconocerlo—, porque en la mayoría de las ocasiones esos hechos no se denuncian. A mi juicio, no se denuncian por tres causas fundamentales. En primer lugar, porque existe un escaso reproche al incumplimiento de la obligación genérica de denunciar que se contiene en el artículo 259 de la Ley de Enjuiciamiento Criminal. Si leemos el artículo 259 de la Ley de Enjuiciamiento Criminal, veremos que la única sanción que lleva aparejado el incumplimiento de la denuncia es una multa de 250 pesetas. En segundo lugar, como policías no podemos forzar a las empresas que han sufrido esos ataques a que nos faciliten los datos. No tenemos ningún instrumento para hacer que el administrador al que me refería venga a denunciar y ponga en nuestro conocimiento los datos o cómo han sufrido los ataques. Estamos hablando de delitos públicos y de daños informáticos indudablemente perseguibles de oficio, pero sin datos no podemos iniciar una investigación. En último lugar, la tercera causa por la que entiendo que existe una predisposición a no formular denuncias es que ni la propia ley que contempla las infraestructuras críticas, la Ley 8/2011, establece esas obligaciones.

Puede haber también otras cuatro razones, quizá ya no de la índole que estamos hablando sino un poco más subjetiva, por parte de las empresas. En primer lugar, las empresas son reacias porque poner una denuncia implica reconocer formalmente un fallo de seguridad en sus propios sistemas y a nadie le gusta que le digan que en su casa han entrado a robar. En segundo lugar, porque como consecuencia de ese reconocimiento los daños de marca o los daños reputacionales que se pueden hacer en la empresa pueden ser bastante importantes. ¿Y por qué no? De acuerdo y conforme a las limitaciones a las que antes me he referido, puede existir escasa confianza en la investigación que hacemos los policías y que llegamos en pocas ocasiones —estoy hablando desde el punto de vista de la empresa— a resultados con éxito. Finalmente, probablemente otro factor que pueda influir es porque los procesos penales suelen ser procesos penales largos en el tiempo y costoso, y eso hace que las empresas de este sector tampoco estén demasiado interesadas.

Como refuerzo de lo que les digo, en el informe de la secretaría de Estado los delitos relacionados con ataques a sistemas informáticos o interceptación de sistemas informáticos se elevan a poco más —si sumamos los dos— de 3600 hechos conocidos por la secretaría de Estado. Sin embargo, los datos de los que dispongo —que son públicos a través del Incibe— son que en 2017 el Incibe gestionó un total de más de 123 000 incidentes relacionados con ciudadanos, empresas e infraestructuras críticas. Es decir, piensen en la diferencia entre esos 3600 y los 123 000 incidentes que gestionó directamente el Incibe. Tenemos puesta la esperanza en el nuevo real decreto-ley que se publicó en el mes de septiembre, el 12/2018, de Seguridad de las Redes y Sistemas de Información que traspone a nuestro derecho interno la directiva Nix que debía haber entrado en vigor. Esa directiva, como ustedes conocen, contiene una serie de obligaciones pero esencialmente en lo que a mí me interesa es por la obligación de notificar incidentes. En el real decreto al que hago referencia ya se habla de obligaciones precisas de comunicar incidentes con independencia —y así lo reconoce el propio artículo 14.3 de ese real decreto— de la obligación formal de presentar la denuncia, según recoge el artículo 259 de la Ley de Enjuiciamiento Criminal. Esos ciberataques se han convertido realmente en la principal amenaza que tenemos ahora los Gobiernos y las

cve: DSCG-12-CM-118

empresas. Me voy a permitir leer simplemente una cifra que da el Foro Económico Mundial, organismo que identifica los ciberataques como el tercer riesgo más importante para 2018 solamente por detrás de las condiciones climáticas adversas y los desastres naturales. Eso es así porque los beneficios —según determinadas fuentes que he manejado— que repercuten a los cibercriminales los podemos cuantificar y determinar en 1,5 billones de euros.

Como les decía, en cada una de mis intervenciones voy a hablarles un poco desde el punto de vista operativa, qué es lo que hacemos frente a esto. Quiero traer a colación una operación de abril de este año en la que detuvimos a un ciberdelincuente que desde la provincia de Alicante a través de la organización —que estaba integrada por una serie de miembros de la mafia moldava— únicamente mandaba un *malware*, un virus para que fueran atacados los bancos rusos y de Taiwán. Este cibercriminal y el grupo al cual pertenecía no atacaban directamente las cuentas privadas de los usuarios o de los clientes de eso bancos sino que atacaban al propio banco. Mediante ese *malware,* que se diseñaba por parte del ciudadano con pasaporte ucraniano al que detuvimos y que actualmente sigue en prisión, se iba escalando una serie de privilegios dentro de los sistemas informáticos del banco hasta el punto de crear cuentas falsas y transferir el dinero del banco mediante dos maneras a las mulas de dinero, que eran quienes lo recogían. La primera manera, con la creación de cuentas y la transferencia de ese dinero iban a cajeros automáticos y como vamos cualquiera de nosotros con nuestra tarjeta de crédito sacaban el dinero del cajero automático previamente engrosado en aquella cuenta corriente. La segunda y probablemente más llamativa, es que atacaban directamente a los cajeros automáticos con un sistema informático diseñado para ello con el que dejaban sin efecto cualquier medida de seguridad que tenía el cajero y el cajero actuaba como una máquina de las que conocemos todos, una máquina tragaperras. Simplemente, echaba y escupía el dinero que estaba dentro del cajero. Nosotros en la investigación tenemos vídeos de cómo las mulas de dinero lo recogen y están fumándose un pitillo mientras esperan a que el cajero empiece a echar ese dinero.

El segundo de los objetivos específicos que se contemplan en el Plan Estratégico Institucional de la Policía ya no está referido al mundo del ciberespacio sino que, probablemente, sea mucho más cercano a nosotros porque está referido directamente a las personas, a los internautas, y a la protección de los más débiles. Del cumplimiento de ese objetivo se ocupa la Brigada central de seguridad informática, que está integrada a su vez por otras dos secciones operativas: una sección operativa de redes abiertas y una sección operativa que lucha contra la explotación sexual infantil por Internet. El porcentaje de delitos conocidos y denunciados relacionados con este segundo objetivo específico de nuestra estrategia solamente alcanza, más o menos, a un 14 % y ahí incluimos las amenazas, las coacciones, los delitos contra el honor y aquellos delitos sexuales que se comenten fundamental a través de la red, pero no de pornografía sino de *grooming* o *sexting*. Para luchar contra ello, tenemos dos pilares fundamentales: por un lado, incrementar el patrullaje activo que se hace a través de la red y las investigaciones que estamos llevando a cabo; por otro, la investigación de la distribución de la pornografía infantil a través de grupos de pederastas o pedófilos.

A nadie se le escapa que ahora mismo el uso de la red nos ha propiciado unas enormes ventajas, unos enormes beneficios, aquellas conversaciones que antaño podíamos tener con nuestros amigos en un bar en las que hablábamos de nuestras aficiones, de nuestras dudas, de si teníamos o no una serie de cosas; ahora, todo ese tipo de comunicaciones se hacen a nivel global directamente desde la red. La red nos permite incluso que aquellas personas que debido a condiciones de timidez o condiciones particulares por las que no son capaces siquiera de emitir cuatro palabras en un foro determinado, simplemente redactando un mensaje y haciendo un clic son capaces de hacer eso que por determinados motivos no eran capaces de hacer en un foro. Indudablemente, la red tiene un componente más dañino que es el anonimato. Incluso desde el anonimato se pueden hacer comentarios, pero además esos comentarios pueden ser de conductas nocivas, conductas alegales o conductas delictivas. Es en este ámbito, en las conductas delictivas, donde entramos nosotros como unidad en funcionamiento. Nosotros como unidad no nos ocupamos ni de las conductas que puedan ser nocivas ni nos ocupamos de esas conductas que son alegales. Únicamente, actuamos —al igual que actúa cualquier policía que podemos ver en la calle— en la red investigando por un lado aquellas conductas de las que hemos tenido constancia por una denuncia o aquellas conductas que, de oficio, vemos que son constitutivas de un delito perseguible de oficio. En este sentido, quiero destacar la preocupación que tenemos en la Policía por la protección de los menores, por la protección de los más débiles.

cve: DSCG-12-CM-118

Nuestro principal esfuerzo en esta área se orienta hacia la detección de una actividad delictiva que es la más repugnante que he visto a lo largo de mi vida profesional. A lo largo de mis treinta y ocho años de vida profesional la más repugnante de las conductas que he comprobado es la conducta de abusos sexuales a menores, la pornografía infantil. El uso de Internet para la distribución de esta pornografía infantil tiene dos efectos fundamentalmente pero que son perniciosos. Es decir, la propia distribución de los contenidos pedófilos implica un motor para que haya más producción de archivos pedófilos. No se conforman simplemente los pedófilos con ver lo que ya tienen sino que están demandando mucho más. Pero lo que quizá sea más importante es que en esos grupos de pedófilos que suelen ser cerrados —blindados, es difícil entrar en ellos— aparte de esa distribución de la pornografía infantil se refuerzan psicológicamente las personas que comparten esos archivos. Si me permiten la expresión, piensan: no soy tan raro, hay más gente como yo que está viendo estos archivos. Pero no piensen que es algo anecdótico, solo el año pasado la unidad que yo dirijo detuvo a 377 personas y abrimos más de 132 investigaciones. Como prueba de ello —en ese ánimo de transmitir la confianza hacia nosotros por parte de ustedes y de los ciudadanos—, les voy a comentar cuatro operaciones, dos de ellas de pornografía infantil y otras dos de la sección de redes. Estamos a punto de cerrar en España y en algún país de la Unión Europea una operación que hemos denominado Telón de acero, en la que se han investigado 806 objetivos en setenta y tres países. La manera de distribuir esa pornografía era a través de la aplicación de mensajería instantánea de Telegram que, como saben ustedes, tiene grandes medidas de seguridad. La esencial nota de interés en esa investigación es que por primera vez estamos actuando con un agente encubierto, evidentemente autorizado por orden judicial. La segunda operación a la que les quería hacer referencia es la Operación Tantalio, que se recogió por la prensa con una gran difusión. En ella desarticulamos noventa y seis grupos de WhatsApp e implicamos a diecisiete países. Hay que destacar que desde la Policía española implicamos a Europol e Interpol para que participaran de una forma conjunta en una *action day,* una acción coordinada, de tal forma que en un mismo día se actuó en Europa, en América Latina y en España.

Con respecto a las redes, hemos desarrollado dos operaciones. Por un lado, la Operación Torre, contra ataques a la salud pública de nuestros ciudadanos. Aquella operación consistió en la detención de más de veinticinco personas que, con una apariencia de representar a farmacias legales, ofrecían a través de Internet medicamentos sin ningún control sanitario, medicamentos que eran fabricados esencialmente en la India y que eran transportados hasta España sin ningún control sanitario. La principal característica de esa operación fue que se intervino un monedero *bitcoin* y que se bloquearon cuentas por valor de más de 320 000 euros. Finalmente, una operación que nada tiene que ver con la pornografía ni con esta Operación Torre o con medicamentos fue la detención este año de cuatro individuos de ideología ultraderechista y neonazi que ponían precio a la cabeza del presidente de una ONG. Los tuits que publicaban eran realmente sorprendentes, simplemente por el hecho de que ese presidente de la ONG era de raza negra.

El tercer objetivo es el fraude informático, como no puede ser de otra forma. Como he dicho antes, el 74,4 % de las infracciones que conocemos se corresponden con los fraudes informáticos. En la lucha contra el fraude informático contamos con dos secciones operativas, una que se ocupa de la lucha contra el fraude en el comercio electrónico, donde estamos implicados todos los ciudadanos con temas tan sumamente conocidos como el incremento de los fraudes relacionados con los alquileres vacacionales de apartamentos, la tarificación adicional de telefónica y las ventas de segunda mano, y otra sección que se dirige directamente a luchar contra el fraude bancario y empresarial. En menos de una década, del 12,8 % de la población que compraba por Internet hemos pasado a un 40 %. Ese incremento es el que posibilita que al mismo tiempo se estén dando estas cifras de las que les hablo. Víctimas podemos ser todos: víctimas particulares, a través de eso que les comentaba de los alquileres, las ventas fraudulentas o los abusos de tarificación telefónica adicional, y también las empresas. De hecho, nosotros cada dos por tres estamos recibiendo alguna denuncia y estamos alertando a la ciudadanía sobre lo que se conoce como el fraude del CEO, que no es otra cosa que, mediante técnicas de ingeniería social, hacerse pasar por el consejero delegado de una empresa y enviar un correo simulando ser ese consejero delegado para engañar a quien tiene disposición económica para que haga una transferencia al grupo criminal. También son víctimas las propias entidades bancarias, puesto que ellos al final son los que tienen que hacerse cargo de esos continuos fraudes que se hacen en las tarjetas de los particulares a que antes me refería.

No podemos pensar que esas acciones se cometen a nivel individual, sino que detrás de cada una de ellas existe una organización criminal, y hemos detectado que al menos confluyen siempre tres tipos

cve: DSCG-12-CM-118

de personas en estas tipologías delictivas. En primer lugar, se utiliza la ingeniería social, alguien que mediante engaño consigue obtener datos confidenciales de aquellas personas a las que quiere atacar. El segundo bloque es el del soporte técnico, es decir en la red Tor, en la red profunda, lo que conocemos como el crimen como servicio, por el que se ofrecen ciberdelincuentes que, a cambio de una contraprestación económica, facilitan a la organización criminal que les pongan a su disposición una herramienta informática que permita que ese ataque pueda realizarse. Y el tercero es un elemento físico, las mulas de dinero. He hecho referencia antes a ellas, son los que aperturan las cuentas bancarias y las que de alguna forma mueven el dinero hasta que llegan a manos de los responsables de la organización.

Siguiendo con esa línea que inicié el principio, voy a hablarles de dos operaciones muy cortas: una de ellas la Operación Valcea, que es una operación por la que detuvimos a treinta y seis personas, fundamentalmente de origen rumano, que lo que hacían era, a través de la publicación de los portales de transparencia de los diferentes contratos que tenían muchas empresas públicas —diputaciones, ayuntamientos—, falsear el destino final de la cuenta a la hora de pagar esos servicios utilizando la propia falsificación y la cuenta para enviarlo al ayuntamiento. Esta operación tiene como característica que se hizo de forma conjunta con los Mossos d'Esquadra. Estuvimos implicados la Policía Nacional de diferentes provincias, estuvo implicada la Policía romana y fue, como he dicho, una investigación conjunta con los Mossos d'Esquadra. La última operación, que probablemente hayan podido ver en prensa la semana pasada, está relacionada con la clonación de tarjetas de crédito, en la que detuvimos a diecinueve personas. El principal cabecilla ya fue condenado por financiar el terrorismo yihadista en los atentados del 11 de septiembre. Con esto creo que les he ofrecido una visión de cómo tenemos la realidad delincuencial en España. Como digo, no es toda la que hay pero sí es toda la que conocemos.

Para finalizar, quería entrar muy brevemente en algunas posibles líneas de mejora que creo que a todos nos ayudarían. En primer lugar, para mí y para nosotros la prevención y la formación es algo esencial. A través del Twitter de la policía estamos permanentemente alertando a los ciudadanos y dándoles consejos sobre posibles fraudes que se están cometiendo y nuevos *modus operandi*, pero necesitamos que eso llegue a más gente. La comunidad educativa, desde mi punto de vista, también se debe de implicar en esa prevención y en la formación. Necesitamos que nuestros jóvenes se incorporen a los planes de estudio. Deben incorporarse medidas para que conozcan el medio cibernético, para que tengan más facilidad y conozcan no solo las ventajas, que son muchas, sino también los riesgos que conlleva. Tanto en la unidad que yo dirijo como en la Unidad Central de Participación Ciudadana ya tenemos contacto directo con colegios, hay un plan director para la convivencia y mejora de la seguridad en centros educativos y se les habla a los jóvenes y se facilitan determinadas campañas. En concreto les podría hablar de dos: «Que el móvil e Internet no te amarguen las vacaciones» y «Está bien saberlo», que no deja de ser una guía que se hizo de manera conjunta entre Google y Policía Nacional poniendo de manifiesto los riesgos que podían suponer. Pero junto a esa labor de enseñanza en los centros educativos por nuestra parte, tenemos además una especial fijación en participar en foros de trabajo y en universidades. Damos cursos de formación a jueces y fiscales, tenemos una estrecha relación con la Fiscalía especial de Criminalidad Informática; estamos permanentemente viajando a Europa para participar y formarnos nosotros mismos sobre las últimas novedades. Es decir, nuestra línea es la prevención y la mejora para concienciar al ciudadano de que tengan un uso de Internet mucho más seguro.

Igualmente, la investigación se configura como una línea de mejora importante. ¿Somos suficientes? Realmente yo tengo el convencimiento de que por parte de nuestra Dirección General hay una preocupación o, mejor dicho, una concienciación por incrementar los recursos de que disponemos en la unidad para ofrecer una mayor respuesta y una mejor investigación a los hechos a los que nos estamos refiriendo. Además de ello, nosotros debemos hacer un esfuerzo adicional porque, como les digo, al no tener fronteras el ciberespacio, debemos acudir a más reuniones internacionales, debemos relacionarnos tanto bilateralmente como con organismos públicos para conocer qué está pasando en otros países y para hacer un intercambio de información fluida.

Finalmente, necesitamos mejorar también nuestras herramientas forenses para hacer los análisis de todos los tratamientos de evidencias digitales que se incautan en los diferentes registros. Pueden imaginar que hoy en día los *pendrives*, el análisis de cuentas de correo, discos duros, todos van a nuestra unidad y hay un grupo especializado que se encarga de ejercer y hacer esos análisis para los investigadores que lo piden. También tenemos necesidad de contar con alguna herramienta que nos pueda certificar digitalmente que un determinado contenido ha sido publicado en una página web. Me consta que por la

cve: DSCG-12-CM-118

secretaría de Estado se está haciendo un esfuerzo en este sentido y están valorando adquirir una herramienta de este tipo para Policía y Guardia Civil.

Necesitamos contar con la empresa del sector público y del sector privado. Mi unidad está participando en dos proyectos de la Comisión Europea del programa Horizonte 2020 llamados Titanium y Ransés financiados con 80 000 millones de euros, y al final se pretende que podamos tener una plataforma que nos permita extraer, almacenar y analizar tanto los *malware* financieros como hacer un seguimiento en relación con las monedas virtuales.

Señorías, con mi intervención lo único que he pretendido ha sido trasladarles sin ningún alarmismo y con un mensaje de confianza la realidad de la ciberdelincuencia y las respuestas que desde la Policía Nacional ofrecemos.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias.

Permítame, en primer lugar, pedir disculpas al compareciente y a todos ustedes por un retraso absolutamente involuntario.

Vamos a empezar sin más dilaciones el turno de intervenciones. Empezamos por el Grupo Confederal de Unidos Podemos-En Comú Podem-En Marea. Entiendo que es el señor Comorera quien toma la palabra.

El señor **COMORERA ESTARELLAS:** Muchas gracias, presidente. Muchas gracias, señor Pérez, por su exposición y por reflejar la problemática que sufrimos en relación con la ciberdelincuencia.

En primer lugar, quería trasladar en nombre de mi grupo parlamentario la felicitación al Cuerpo Nacional de Policía, y en especial a la Unidad Central de Ciberdelincuencia, por las operaciones que nos ha relatado aquí. Hace poco tuve el placer de estar en la sede de Europol en La Haya y realmente me llevé una grata sorpresa por los muchos policías y guardias civiles que allí trabajan y la buena fama que tiene en Europa nuestro trabajo en términos de ciberdelincuencia. Quiero trasladárselo.

En anteriores intervenciones suyas siempre dice que hay tres retos esenciales para la policía que son los grupos de ciberinteligencia, el patrullaje activo y la lucha contra las estafas y el comercio *online,* donde se está observando un incremento de actividad delictiva, tal y como ha reflejado con los datos que nos ha facilitado ahora. El patrullaje activo dentro de un mundo inabarcable que podríamos decir que es el mundo de Internet, tanto en fuentes abiertas como en la Internet profunda, realmente es muy complicado. Entrando un poco en su último mensaje, ¿cree usted que los medios personales y técnicos actuales con los que cuentan son suficientes para realizar ese patrullaje activo que dice que debería ser un reto esencial? Muy relacionado con ello, ¿cree que es suficiente lo que se dedica presupuestariamente a esa formación o cree que es necesario aumentar la formación respecto a las nuevas tecnologías y el desarrollo de las mismas de las Fuerzas y Cuerpos de Seguridad del Estado? En esta misma Comisión la fiscal de sala coordinadora en materia de criminalidad informática nos decía que había que invertir seriamente en formación a distintos niveles y también que había que dotar de medios personales y materiales a las unidades de investigación y a los laboratorios de policía científica y de criminalística.

Otro problema evidente con el que se encuentran es con la transversalidad de los delitos al utilizar las nuevas tecnologías, la internacionalización o colaboración entre las partes y la dificultad de tener que solicitar información a las empresas tecnológicas radicadas en el extranjero. La pregunta es: ¿cree usted que es suficiente para el éxito de su trabajo el marco legal establecido en la ratificación en su día del Convenio de Budapest y las reformas de 2015 del Código Penal y la Ley de Enjuiciamiento Criminal o tendríamos que ir más allá?

Como ya ha dicho usted, legislativamente siempre vamos detrás del avance de la teología. Uno de los temas que preocupan por la escasez de regulación es el de las criptomonedas, lo que imagino que es un hándicap en sus investigaciones. Las ICO y el *cryptojacking,* cada día surgen nuevas formas que podrían ser delictivas. Desde el punto de vista policial, ¿qué cree que tendríamos que hacer legislativamente al respecto en relación con las criptomonedas?

Una de sus críticas o frustraciones que he visto en alguna de sus intervenciones, como ha expuesto hoy aquí, es la falta de denuncias, en especial de empresas en sectores estratégicos como puede ser el turismo, la sanidad o incluso los juguetes infantiles. En concreto, y según datos que usted ya ha facilitado, según el Incibe, en 2017 ha habido 123 624 incidencias, de las cuales 116 000 afectaron a ciudadanos y empresas y solo fueron denunciadas 66 500, si he visto bien los datos. ¿Cree que hemos avanzado algo en esto? Evidentemente, la Directiva NIS y el real decreto son un avance, pero

cve: DSCG-12-CM-118

¿realmente han perdido el miedo o las reticencias las empresas por la pérdida reputacional que supone el reporte de este tipo de ciberataques? ¿O cree que realmente necesitaríamos una reforma del artículo 259, como me ha parecido entender, de la Ley de Enjuiciamiento Criminal para reforzar que las empresas denuncien estos hechos?

Le agradecería que nos dijera cómo definiría la colaboración actual con la justicia y con la fiscalía especialmente y, en su caso, en qué cree que debería mejorarse en este apartado. A este respecto, me gustaría que desde su experiencia nos dijera cómo juzgaría el entendimiento con la justicia, y lo digo a nivel de formación, por ejemplo, de la judicatura, pues me constan las dificultades que tienen en muchas ocasiones para explicar cosas muy básicas en los juicios orales, por ejemplo, para hacerse entender o sobre el tipo de pruebas propuestas en ocasiones porque muchas veces los propios jueces que tienen que dictar algún auto para intervenir de alguna forma no entienden lo que ustedes muchas veces les intentan explicar. Me ha llegado, sobre todo por parte de fiscalía, que muchas veces tienen problemas, y lo ligaríamos un poco a la formación que antes había comentado.

Me gustaría saber si tienen algún sistema de control en cuanto a los delitos o las infracciones leves, sobre todo en relación con las estafas, que permita establecer relaciones entre unos y otros porque nos preocupa mucho que a veces pequeñas estafas que no llegan a las cantidades requeridas para seguir como delito queden muy difuminadas, a pesar de que detrás, como ha comentado, muchas veces existen verdaderas organizaciones criminales.

En cuanto a los delitos de odio a través de las redes sociales, me gustaría saber qué criterios siguen ustedes, qué se persigue y qué no se persigue. Los que estamos acostumbrados a navegar por las redes nos damos cuenta de que no es difícil encontrarse con algo que podría ser considerado muchas veces delito de odio. Pero es imposible, evidentemente, ponerse a perseguirlo todo. Por tanto, me gustaría saber qué criterio sigue la policía para determinar qué que persigue y lo que no.

Para finalizar, en cuanto al tema de ciberdelincuencia, me gustaría saber cómo valora la colaboración con otros cuerpos policiales, con la Guardia Civil y con policías autonómicas, incluso locales.

Muchas gracias.

El señor **PRESIDENTE:** Gracias, señor Comorera.

Señor Hernando.

El señor **HERNANDO VERA:** Gracias, señor presidente.

Enhorabuena, señor comisario, por su intervención, que ha sido clara y concisa y nos ha ilustrado sobre la eficacia de la unidad que usted dirige. Reitero lo que ha dicho mi antecesor en el uso de la palabra; enhorabuena y felicidades a usted, a todo su equipo, a toda su plantilla, por las operaciones que han llevado a cabo y por su eficacia, que es la que nos hace a los ciudadanos tener confianza en su trabajo. Por eso, el mensaje que usted ha lanzado genera en mi grupo confianza en la eficacia de su unidad y, en general, en la Dirección General de la Policía.

Usted ya habrá visto, porque ha leído las intervenciones de sus antecesores, de otros expertos en la materia, que en esta Comisión hay una serie de clásicos modernos: está, en principio, la reivindicación que hacen todos ustedes, lógica, de más y mejores medios, de medios más actualizados, porque las tecnologías avanzan y los malos avanzan muy rápido, y está la necesidad de coordinación —se hacía ahora mismo mención a la palabra estrecha— entre cuerpos policiales. He visto también su importante colaboración con cuerpos policiales no españoles, con cuerpos de otros países, como, por ejemplo, en la Operación Worldcom con la Policía china. En este sentido, le pregunto cómo sería posible mejorar esa colaboración con cuerpos policiales de otros países en una serie de delitos en los que precisamente la ubicuidad y la trasnacionalidad son una de sus notas características, así como la coordinación con los distintos estamentos del mundo de la ciberseguridad que trabajan de distinto modo.

Voy a reiterar algunas preguntas, sin ánimo de cansarles. Reformas legislativas. ¿Usted piensa que es necesaria alguna reforma legislativa concreta después del Real Decreto para la trasposición de la Directiva NIS y después de la reforma de la Ley de Enjuiciamiento Criminal? Nos ha hablado, por ejemplo, de la importancia del agente encubierto en esas actuaciones contra esos crímenes execrables de pedofilia y pornografía infantil. ¿Piensa que desde esta Comisión podríamos solicitar, impulsar y recomendar alguna medida legislativa nueva, novedosa, pero necesaria, para mejorar su eficacia?

Formación y perfiles. Una de las cuestiones a la que nos hemos enfrentado en la Comisión es la necesidad de perfiles muy técnicos. ¿Cuáles son los perfiles más demandados, más necesarios, los que ustedes necesitan especialmente a la hora de investigar este tipo de crímenes? Sabemos que en su

cve: DSCG-12-CM-118

unidad hay ingenieros, matemáticos, físicos y técnicos informáticos. ¿Qué tipo de perfiles están demandados y son necesarios por parte del mundo educativo para atender sus necesidades?

En el mundo de las criptomonedas, al que también se ha hecho referencia, y dada la complejidad y opacidad del propio medio, ¿tienen más problemas con las estafas que se hacen con las criptomonedas o con los problemas de blanqueo de capitales a través de las criptomonedas? Son dos de las posibilidades más habituales en relación con la ciberdelincuencia y las criptomonedas.

Por último, cifras. Nos ha dado cifras del año 2017 y estamos en el último trimestre de 2018. ¿Nos puede adelantar, en cifras, lo que está pasando este año, sobre todo respecto a la eficacia? También me gustaría saber si la ciudadanía colabora con ustedes en la detección y denuncia de determinado tipo de delitos, como ese tan execrable del que hemos hablado, la pedofilia, y si también lo hacen las empresas de Internet, empresas que gestionan, por ejemplo, redes sociales, como Twitter o Instagram. ¿Cómo podemos mejorar esa colaboración ciudadana? ¿Colaboran con ustedes de manera eficaz las grandes empresas que gestionan estas redes sociales y que, por cierto, no tienen su sede en España mayoritariamente?

Por mi parte, nada más. Muchas gracias y, de nuevo, le reitero la enhorabuena, que hago extensiva a todos los miembros de su equipo.

Gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Hernando.

Señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Muchas gracias, señor presidente.

Agradecemos la comparecencia de don Rafael Pérez, cuya intervención ha sido exhaustiva, concreta y muy ilustrativa con respecto a su unidad, que comenzó en el año 1995 con cuatro funcionarios y que hoy tiene más de cien, y a esas magníficas operaciones de las que ha hecho gala aquí. Ayer mismo recibía yo una respuesta del Gobierno, por lo que tengo que felicitar de nuevo a la policía por ese plan director respecto al ciberacoso escolar que puso en marcha la secretaría de Estado junto con la Policía y la Guardia Civil, pues los datos reflejan que se va mejorando en este tema, y todo gracias al trabajo que hacen ustedes. En España, hemos pasado de tener cincuenta y ocho casos de ciberacoso escolar en 2012 a tener veintiocho, y en Ourense, que es mi provincia, de tener tres casos a no tener ninguno durante dos años. Creo que esas charlas que vienen dando por los colegios, más de dos mil de media al año, son productivas y los datos están ahí.

En esta Comisión somos conscientes de que las nuevas tecnologías e Internet son motores de competitividad y de prosperidad. Las oportunidades económicas y sociales están a nuestro alcance gracias a las tecnologías. Pero también somos conscientes de nuestra dependencia tecnológica y de la vulnerabilidad a la que nos enfrentamos en este momento en el ciberespacio. A las amenazas de seguridad por tierra, mar, aire y espacio, ahora hay que incluir las del ciberespacio. Nos daban un dato en una de las comparecencias: cada treinta y nueve segundos se produce un ciberincidente en España. Eso no tiene que alarmarnos, pero los legisladores tenemos que crear la conciencia de ciberseguridad en la sociedad, es necesario. Hasta hace pocos años la sociedad en general no era consciente del problema que existía, ni tampoco lo eran las empresas. Yo creo que el WannaCry, con 360 000 equipos afectados en ciento ochenta países, marcó un antes y un después, y el ejemplo es que se ha creado esta Comisión. Me quedo con la idea que usted decía —y tiene toda la razón— de que los legisladores vamos por detrás. En Estados Unidos ya tenían una estrategia de ciberseguridad en 2009 y nosotros hasta 2013 no la hemos puesto en marcha. ¿Que si creo que debemos de ir por delante? Por supuesto.

Le quería hacer algunas preguntas. Esto de intervenir en último lugar facilita las cosas porque ya las han hecho los demás, y hoy coincido más con los de Podemos que con los del PSOE en las preguntas; será por eso de que ya estamos en la oposición. Nos preocupa mucho el tema de la comunicación de los ciberincidentes por parte de las empresas y el coste reputacional que les supone, que es por lo que no se comunican. La Directiva NIS y este Real Decreto 12/2018 establecen la obligatoriedad de comunicarlos y las sanciones a las que se pueden enfrentar. Pero cuando nos reunimos con ellas nos dicen que echan en falta una plataforma unificada de notificación de incidentes; es decir, no tener que andar comunicando los incidentes en varias ventanillas sino tener una plataforma. El Grupo Popular va a proponer una enmienda en este sentido para facilitar las cosas, es decir, para no solo exigirles que realicen la comunicación, sino también para facilitarles esa comunicación. Tampoco está todavía bien establecida en este decreto la colaboración público-privada. Los legisladores debemos de hacer hincapié en esa

cve: DSCG-12-CM-118

colaboración, al igual que con la figura del notificante, no vaya a ser que tengamos notificaciones falsas, no veraces, y que metamos en problemas a empresas. Eso lo debemos observar en el real decreto.

Me gustaría hacerle una pregunta sobre los medios que en concreto usted dijo que echaba en falta. Es decir, ¿son medios técnicos o medios personales? Porque últimamente es verdad que el Cuerpo Nacional de Policía, al igual que la Guardia Civil, han sufrido los efectos de la crisis con unas promociones muy pequeñas; la última ha sido ya bastante grande, con más de tres mil efectivos, y querría saber si se refiere a medios personales o a medios materiales, o a ambos, y si nos podría concretar algo más al respecto.

También ha hablado de pasada en alguna de las operaciones de la figura del agente encubierto. Aquí alguno de los comparecientes nos ha propuesto la modificación de este agente encubierto. Me gustaría saber si cree usted que es suficiente o si debemos legislar para actualizar esta figura. Asimismo, me imagino que por la investigación de los delitos pueden tener criptomonedas incautadas, y me gustaría saber si las tienen y qué hacen con ellas, en estos momentos en los que no existe una legislación en España al respecto.

Aquí en esta Comisión se está hablando sobre la ciberreserva o el cooperador en ciberseguridad, nosotros vamos hablar de este último, como es el caso de Francia, Reino Unido, Alemania o Estados Unidos. En algunos sitios, como Francia, la Policía tiene un cooperador en ciberseguridad que va a dar charlas a los colegios, y quisiera saber si echan en falta ese cooperador en ciberseguridad. En el caso del WannaCry dicen que fue un cooperador en Reino Unido quien dio con el efecto, con el arma que paralizó ese ataque del WannaCry. ¿Cómo valoraría usted un cooperador en ciberseguridad en las Fuerzas y Cuerpos de Seguridad del Estado, en este caso en la Policía que es más civil? Por otro lado, también hay un delito, que no es delito, porque según nos decía un compareciente no está regulado, pero nos gustaría saber si han notado, sobre todo por las ciudades, que es donde ustedes tienen la demarcación, el *cryptojacking,* y si han visto si esto ha ido en aumento. No sé si ha tenido conocimiento de más casos. A nosotros nos hablaban de que en los últimos meses, desde mayo, se suceden este tipo de casos y querría saber qué podríamos hacer nosotros como legisladores al respecto. Es verdad que no se usa físicamente el terminal de esa persona, pero sí se está usando remotamente hasta que causa una explosión, o arde, etcétera.

En cuanto al tema de la identidad digital, querría saber si usted cree que los legisladores deberíamos dar un paso más allá para facilitar que no haya tanto cibercrimen, que no haya tantos ciberataques, y si deberíamos facilitar en las redes también, cuando nos damos de alta —estoy pensando en el ciberacoso—, regular más la identidad digital, porque creo que muchas veces los perfiles son falsos y posiblemente detrás de un niño está un señor adulto, y lo hemos visto cantidad de veces. Por lo tanto, ¿deberíamos dar un paso más y regular la identidad digital?

Creo que el señor Hernando y yo, que llevamos muchos años trabajando en temas de Interior, coincidimos en muchas cosas, sobre todo en el apoyo a las Fuerzas y Cuerpos de Seguridad del Estado, y sé que leyó la misma entrevista que yo en el periódico *ABC, Los patrulleros de la red,* que comenzaba: «Ingenieros, matemáticos, físicos, técnicos informáticos...», y yo me quedo, porque lo traía subrayado, con esta frase: «Policías con amplio bagaje y con olfato».

Nada más y muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señora Vázquez.

Señor comisario.

El señor **COMISARIO PRINCIPAL DE LA POLICÍA NACIONAL Y DIRECTOR DE LA UNIDAD CENTRAL DE CIBERSEGURIDAD** (Pérez Pérez): Gracias, señor presidente.

Son demasiadas preguntas, no sé si voy a ser capaz de contestar a todas y en el orden en que me las han formulado.

En cuanto a si los medios son suficientes, pues nunca son suficientes los medios, indudablemente, eso es una obviedad; tenemos los que tenemos. Yo puedo estar ligeramente satisfecho, porque cuando llegué a la unidad estaba integrada por unos 70 o 72 funcionarios de Policía y ahora la integramos creo que son 104 o 106; es decir, no tenemos suficientes medios, nos gustaría tener más, pero es lo que hay; con las limitaciones es lo que hay. Sí le puedo decir, como lo he hecho a lo largo de la comparecencia, que me consta que por parte de la dirección hay una concienciación y una preocupación sobre este tema, tanto en medios materiales como en medios humanos.

cve: DSCG-12-CM-118

En cuanto a invertir en formación, los planes de formación del Cuerpo Nacional de Policía no los diseño yo, le corresponde a la División de Formación y Perfeccionamiento diseñar esos planes de formación y formar a nuestros alumnos en Ávila. Pero bien es verdad que más que invertir en formación, yo le daría la vuelta y deberíamos invertir en talento; es decir, recuperar a aquellos alumnos que salen en Ávila bien como policías o bien como inspectores del Cuerpo Nacional de Policía, Policía Nacional, recuperar ese talento para que fuera utilizado ahí. Eso yo creo que no cuesta dinero, es prácticamente gratis.

No sé si es que ha visto alguna presentación mía, cuando me habla de que yo hablo de turismo, de juguetes, etcétera, porque efectivamente yo suelo situar al personal con una serie de imágenes, y efectivamente hablo de los juguetes, hablo de la seguridad en empresas farmacéuticas, y entonces no sé dónde lo ha podido ver. Me decía algo sobre que si genera miedo, no le entendí bien porque apunté la palabra miedo. **(El señor Comorera Estarellas: El miedo reputacional de las empresas a la hora de denunciar).** Pues hombre, yo tengo sincera esperanza en que la entrada en vigor del Real Decreto-ley 12/2018, a la que antes he hecho referencia, ha empezado a andar, y tengo confianza y esperanza en que eso nos produzca, primero, una concienciación en las empresas, que luego repercuta indudablemente en las Fuerzas y Cuerpos de Seguridad del Estado a la hora de que nos pongan en conocimiento determinadas actuaciones. No podemos olvidar que policialmente eso nos va a permitir no digo siempre, pero sí tener conocimiento de lo que ocurre, poder avisar, poder investigar y evitar, en muchos casos, que eso siga ocurriendo en otras empresas. Para mí es esencial ese conocimiento, porque nos aporta esa información que nosotros necesitamos a la hora de abordar el problema.

Hablaba también de la colaboración que tenemos con la justicia y con la fiscalía. Yo le puedo decir que es una colaboración, si me permite la expresión, extraordinaria. Yo, con la Fiscalía especial de Criminalidad Informática, hablo frecuentemente. Ahora hemos perdido una fiscal; me imagino que pronto la recuperarán, e indudablemente con los jueces que nos llevan y que nos instruyen las causas los operativos hablan de manera directa y constante y les exponen, indudablemente, cuáles son las preocupaciones y por dónde debemos ir. Los jueces lo entienden y tenemos una extraordinaria comunicación, hasta el punto de que nosotros hemos participado —como les he referido, aunque fuera de pasada— en la formación de jueces y fiscales, en jornadas que organiza la propia fiscalía, tanto para sus fiscales delegados territoriales en criminalidad informática como para los fiscales en general, incluso en el Consejo General del Poder Judicial.

En cuanto al sistema de control de estafas y lo que me decía de las estafas pequeñas, lo cierto es que nosotros tenemos un sistema de control a nivel interno policial; no es el que se recoge en el sistema estadístico de criminalidad, donde todos los hechos que se denuncian en cualquier comisaría, no solo de estafas, van a una aplicación informática y ahí están. Sí tenemos conocimiento de que este año también se ha producido un incremento en las denuncias de esas estafas. Lo que no le puedo asegurar es si ese incremento está directamente relacionado con una organización criminal que hay detrás, o también puede ser como consecuencia de que cuando a nosotros nos hacen un cargo indebido en nuestra tarjeta el banco nos exige que vayamos a la Policía a denunciar. Es decir, eso puede tener una explicación de por qué ese incremento de las estafas.

Me preguntaba sobre qué criterios seguimos en los delitos de odio. Pues el criterio que nos marca el Código Penal; nosotros no actuamos con ningún otro criterio. El Código Penal establece una serie de tipificaciones; si nosotros entendemos que entra dentro de esa tipificación, tratamos de judicializarlo, y es el único criterio, el que nos marca el Código Penal.

En cuanto a la colaboración con otros cuerpos policiales, yo creo que colaboramos entre nosotros y que no tenemos ningún problema. He hecho referencia a lo largo de mi comparecencia a que en una operación de tanta envergadura como fue la Operación Valcea tuvimos relación directa con un cuerpo de Policía autonómica como eran los Mossos d'Esquadra. Con las policías extranjeras tampoco tenemos ningún problema. Nosotros hemos llevado a cabo operaciones directamente relacionadas y hemos intercambiado información con el FBI, con la Policía alemana, con la Policía holandesa o con la Policía italiana. Las operaciones a las que yo hacía referencia relacionadas directamente con pornografía infantil afectan a otros países. Es decir, esos grupos de pederastas no funcionan única y exclusivamente en España, sino que funcionan también en otros países.

Me preguntaba si el presupuesto era suficiente. El presupuesto no lo determino yo. La Dirección General de la Policía o el Ministerio del Interior reciben un presupuesto y en virtud de las necesidades —porque es verdad que todos pedimos— se asigna y se racionaliza en función de lo que le corresponde a cada uno. Como le digo, ni el presupuesto ni los medios son nunca suficientes, no ya en mi unidad sino en general, pero esta es una cuestión que no me corresponde a mí. Creo que no me he dejado ninguna de las preguntas en el tintero.

cve: DSCG-12-CM-118

Señor Hernando, en cuanto a mejorar la colaboración y la coordinación entre los diferentes estamentos, como le he dicho, nosotros mantenemos una relación extraordinaria con otros países extranjeros y dentro de España mantenemos colaboración con las empresas proveedoras de servicios, con las empresas del sector estratégico, aunque nada más sea a nivel de intercambio de información, que no de denuncia. En cualquier caso, aunque la colaboración es siempre mejorable, yo creo que no tenemos ningún problema en colaborar con las empresas ni las empresas en establecer mecanismos de coordinación con nosotros.

¿Qué reformas legislativas necesitaríamos? Yo creo que la referencia que he hecho a la Ley de Enjuiciamiento Criminal es significante en el sentido de que, por ejemplo, todavía estemos hablando de 250 pesetas y no exista un reproche penal ante el incumplimiento genérico de la obligación de denunciar, pero no me corresponde a mí decidir la política de modificaciones legislativas.

En relación con las criptomonedas, las estafas y el blanqueo, quiero señalar que el dinero de las estafas sí puede convertirse en criptomonedas y utilizarse luego para blanquear, pero del blanqueo se ocupa la Unidad de Delincuencia Económica y Fiscal de la Comisaría General y no la Unidad Central de Ciberdelincuencia. Sí que es cierto —y el ejemplo lo he puesto cuando he hablado de la Operación Torre— que prácticamente todo el dinero que se incautó se incautó en *bitcoin* y se puso a disposición del juzgado.

En cuanto a cifras, les puedo decir lo que estamos haciendo. En fraudes tenemos abiertas ahora mismo 1907 investigaciones, de las cuales 572 han dado resultado y llevamos 600 detenidos, y no hablo de secretaría de Estado sino de la Dirección General de la Policía; en protección al menor llevamos 298 investigaciones cerradas con 309 detenidos; en seguridad lógica, los ciberataques a los que hacía referencia, llevamos 28 investigaciones con resultado y 49 detenidos, y en redes abiertas llevamos 55 investigaciones con resultado y 75 detenidos. Es decir, yo creo que estamos dando una respuesta acorde a exigencia.

Finalmente, me preguntaba por la colaboración de empresas como Twitter o Instagram. Como usted sabe, todas estas empresas radican fuera de España y lo que hacemos cualquiera de nosotros al ser usuarios de esa red social es aceptar las condiciones de uso que la empresa nos marca, y automáticamente, aceptando esas condiciones de uso, creo recordar que solamente hay una excepción, en el caso de Alemania, pero en el resto de los casos todos nos sometemos de manera implícita a la jurisdicción del país donde radica. Sí contamos con su colaboración, pero indudablemente en la mayoría de las ocasiones cuando se la pedimos nos solicitan un mandamiento judicial para poder proporcionarnos una IP o una identidad de la persona. Es cierto que si en alguna ocasión entienden que no se trata de un delito, solicitan una comisión rogatoria internacional que se tramita a través del juzgado correspondiente.

Señora Vázquez, me hablaba de que las empresas del sector privado exigen una plataforma única. En este sentido, lo único que le puedo decir es que dicha plataforma única se canaliza a través del Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad y de la Oficina de Coordinación Cibernética, como órgano técnico del Ministerio del Interior. Es decir, son ellos los que pueden recibir esos incidentes. A partir de ahí sí podemos establecer mecanismos de coordinación interna entre nosotros para que nos comuniquen a Policía y a Guardia Civil esos conocimientos.

En cuanto a los medios, yo no he dicho en ningún momento que eche en falta medios; digo que, como todo, habría que mejorarlos, como le he contestado a su compañero, porque todo es mejorable. Es decir, jugamos en el equipo en que jugamos y tenemos los medios que tenemos, y en este sentido no somos como los entrenadores de fútbol, que con dinero podemos comprar más o menos, sino que tenemos exactamente lo que tenemos y con eso tenemos que ganar la partida. Yo creo que si no la estamos ganando por lo menos estamos dando pasos muy importantes para avanzar en toda esta delincuencia que a nadie se le escapa que es nueva. No se trata de una delincuencia tradicional, como cuando yo ingresé como inspector de Policía allá por el año ochenta.

Desconozco cuál es la propuesta que se hace del agente encubierto, si va a mejorar o va a empeorar lo que hay actualmente. Ahora mismo a nosotros nos está funcionando. Es decir, nosotros hemos ido al juzgado, hemos presentado las evidencias que tenemos, hemos pedido la utilización de un agente encubierto y el juez nos ha dado el oportuno auto por el cual nos autoriza a actuar como agente encubierto. Insisto en que desconozco cuál es el contenido y si esta cuestión mejoraría o no, pero de momento todo lo que suponga mejorar será bienvenido por nuestra parte.

En cuanto a la ciberreserva, como usted sabe, no me corresponde a mí decir cuál es la división de personal, pero es verdad que por mi mentalidad de policía, aunque ahora este en el ámbito de la Policía cibernética, le puedo decir que la Policía siempre ha contado con colaboradores y con personal

cve: DSCG-12-CM-118

cooperador, por tanto, no sé por qué no va a seguir ocurriendo exactamente lo mismo. Otra cosa es que se integre dentro de la Policía, aquí ya hablamos de cosas diferentes, pero en cuanto a colaboradores o cooperadores, por parte de la Policía desde luego no tenemos ningún problema a la hora de que alguien nos ayude a enfrentarnos de una forma más eficaz a todo esto. Finalmente, como digo siempre, tenemos capacidad y voluntad para actuar, pero necesitamos que nos ayuden a ejercer dicha capacidad y dicha voluntad.

El señor **PRESIDENTE:** Muchísimas gracias, comisario.
¿Alguna precisión por parte de los grupos? **(Denegaciones).**
Se levanta la sesión.

Eran las dos de la tarde.

cve: DSCG-12-CM-118