DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2017 | XII LEGISLATURA | Núm. 54 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 8

celebrada el jueves 28 de septiembre de 2017 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

---

cve: DSCG-12-CM-54

Se abre la sesión a las cinco y diez minutos de la tarde.

El señor **PRESIDENTE:** Empezamos la comparecencia. Comparece don Joaquín Castellón Moreno, director operativo del Departamento de Seguridad Nacional, para informar sobre diversas cuestiones relativas a la ciberseguridad en España.

Director, tiene la palabra.

El señor **CASTELLÓN MORENO** (director operativo del departamento de seguridad nacional): Muchas gracias, presidente.

Señorías, en primer lugar, quería manifestarles el honor que es para mí comparecer ante todos ustedes, fundamentalmente por dos motivos. En primer lugar, por la importancia del tema de la ciberseguridad. La ciberseguridad, como ustedes conocen, es un ámbito de especial interés declarado en la Ley 36/2015, de Seguridad Nacional. En segundo lugar, porque me permitirán que, en mi modesta opinión, considere que la creación de esta Comisión Mixta de Seguridad Nacional es uno de los grandes logros de la Ley de Seguridad Nacional a la que antes me refería. Creo que es importante que un tema como la ciberseguridad tenga un espacio natural en el Parlamento para que ustedes puedan estar lo mejor informados posible al ser piezas claves de la política de seguridad nacional y de la política de ciberseguridad en España.

El propósito de mi intervención, señorías, dado que tengo la responsabilidad y el privilegio de ser el primer compareciente en esta ponencia, es trazar el estado de la ciberseguridad en España, algo que realizaré desde la perspectiva del director operativo del Departamento de Seguridad Nacional que, como ustedes saben, es un órgano de asesoramiento del presidente del Gobierno y de la Secretaría Técnica del Consejo de Seguridad Nacional. En esta condición he participado desde el año 2012 —año en que se crea el Departamento de Seguridad Nacional— en los trabajos conducentes a la puesta en pie de la arquitectura político— estratégica de lo que hoy en día se articula el sistema de ciberseguridad en España. A este fin, organizaré mi intervención en torno a cuatro grandes puntos. Trataré, en primer lugar, la singularidad y complejidad del ciberespacio y las acciones negativas que en este dominio se realizan. Sobre esta base, me referiré al modelo que en España se ha ido desarrollando para hacer frente a las ciberamenazas, con especial atención a su dimensión orgánica. A continuación —porque en el ciberespacio es verdad absoluta que no hay límites ni fronteras; la seguridad interior y exterior se juntan— hablaré de algunas iniciativas internacionales en las que España participa. Concluiré, señorías, con una referencia a tres cuestiones de la mayor trascendencia de cara al futuro desde el punto de vista del Departamento de Seguridad Nacional. Estas tres cuestiones son: gestión de crisis, cultura de ciberseguridad y colaboración público-privada en este ámbito.

La Estrategia de Seguridad Nacional del año 2013, cuyo proceso de elaboración fue coordinado por el Departamento de Seguridad Nacional, destacaba la relevancia de dos amenazas, tanto por la probabilidad de que ocurriesen como por su impacto. Me refiero al terrorismo internacional de carácter yihadista y a las ciberamenazas. Identificadas las amenazas y su perfil de evolución, fue necesario definir las líneas de acción y disponer de los medios para hacerles frente. Con algo de paradoja se constató que en España, después de muchos años de lucha contra el terrorismo, habíamos desarrollado unas excelentes capacidades en este terreno, pero que la situación era muy diferente en el caso de la ciberseguridad. Podríamos decir que nos encontrábamos ante un edificio que comenzaba su construcción, situación por lo demás similar a la de los países de nuestro entorno. Cabría preguntarse, entonces, por qué se producía este fenómeno, por qué a cualquier amenaza había, de repente, que anteponerle el prefijo ciber. Casi sin darnos cuenta nos encontrábamos en el mundo del ciberterrorismo, del ciberespionaje, de la ciberdelincuencia o del ciberfraude. La razón fundamental es la propia naturaleza del ciberespacio, un espacio que ha evolucionado a una enorme velocidad, ofreciendo innumerables posibilidades al progreso y al desarrollo de la sociedad pero, a su vez, con grandes lagunas desde el punto de vista de la seguridad. Hoy en día el ciberespacio es considerado, junto con los océanos, el espacio aéreo y el espacio ultraterrestre, como un denominado *global commons,* que son espacios comunes que conectan el mundo, permiten el libre flujo de personas, bienes, información, servicios e ideas. Sin embargo, son espacios de débil legislación, difícil control, de fronteras difusas y que ofrecen, además, un alto grado de mimetismo. Es decir, son espacios propicios para la propagación de amenazas, donde la probabilidad de éxito es alta y el riesgo es muy bajo. La tecnología avanza de forma exponencial pero, frecuentemente, no viene acompañada de medidas de seguridad que garanticen un desarrollo seguro y fiable. Digamos que se ha primado la conectividad en detrimento de la seguridad. Esta situación,

cve: DSCG-12-CM-54

unida en el caso del ciberespacio al fenómeno de la hiperconectividad, amplía nuestro nivel de exposición a las ciberamenazas, amenazas que continúan aumentando en número, alcance y sofisticación. Quizá uno de los aspectos más preocupantes en el entorno de la ciberseguridad es la dificultad de la atribución de las acciones ilícitas. Descubrir quién está detrás de un ciberataque es una tarea ardua que en escasas ocasiones tiene buen resultado. Hay dos elementos que lo explican: la propia complejidad del espacio virtual, altamente tecnológico, y la difícil trazabilidad de las acciones en este medio. La navegación en Internet y el adentramiento en el ciberespacio suponen el acceso a múltiples redes y sistemas conectados entre sí de muy diversos países. Conocemos el punto de partida pero desconocemos, en cambio, la ruta, la singladura, el puerto de llegada e incluso qué alojará nuestro equipaje al regreso. Por citar un ejemplo, los centros de procesos de datos de Google están repartidos por todo el mundo: en Estados Unidos, en Asia, en Europa o en América del sur. Igual pasa con Facebook o Twitter. Además, la navegación casi siempre es dinámica y se pasa de una dirección a otra; todo ello sin detenerme ahora, señorías, en los métodos de navegación oculta o de cifrado de las comunicaciones, que todavía dificultaría mucho más todo este proceso de navegación.

Estas circunstancias explican la difícil atribución de las acciones que se realizan en el ciberespacio. Ante un incidente de ciberseguridad, no es suficiente con disponer de las evidencias técnicas, ya que esta información suele estar falseada o muchas veces nos conduce a error al atribuir acciones a terceras partes no involucradas. Son precisas acciones de investigación en profundidad, en inteligencia, de evidencias adicionales a fin de detectar los patrones de conducta y, aun así, muy raramente llegaremos a atribuir cien por cien un acto ilícito en el ciberespacio. Así, por ejemplo, en los recientes ciberataques del WannaCry o del Petya, a pesar de disponer de numerosa información técnica sobre el comportamiento del *malware* utilizado, no se ha podido atribuir fehacientemente la autoría. Cabe traer a colación, sin embargo, algunos casos de éxito, como la actuación coordinada entre el FBI y Europol, en julio de 2017, que pudo cerrar dos de las grandes páginas de venta de productos ilegales en la denominada red oscura o *dark web*. Estas dos empresas son AlphaBay y Hansa, donde se vendían desde drogas y armas hasta *malware* para realizar ciberataques.

Antes de continuar, permítanme, señorías, un pequeño paréntesis para aclarar lo que entendemos por ciberseguridad. Se incluye dentro de la ciberseguridad todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos, que es importante. Por el contrario, aquellas acciones que en cambio utilizan, por las características del medio, fundamentalmente su conectividad para ejercer campañas de influencia, de daño reputacional, etcétera, pero no llevan una alteración tecnológica, no son consideradas en sí ciberseguridad aunque, desde luego, son acciones ilícitas en contra del uso legal y seguro del ciberespacio. Pongo algunos ejemplos para diferenciar ambos escenarios. Es importante, señorías, trazar esta distinción. ¿Por qué? La respuesta en uno u otro caso son distintas y necesitan tratamientos diferentes que comprometen en su solución a actores diferentes. Los ciberataques más comunes incluyen los ataques de *ransomware,* que se han cuadriplicado desde 2016, denegación de servicio, robo de datos, sabotaje digital, desfiguración de páginas web, *hackeo* de dispositivos móviles, espionaje, acciones delictivas con fines terroristas o criminales. El informe Internet Organised Crime Threat Assessment, de 2017, que publicaba ayer precisamente Europol, destaca en concreto que los ataques de *ransomware* son la mayor ciberamenaza por su variedad, alcance y daño. Indica, igualmente, que se han filtrado más de 2000 millones de datos relacionados con ciudadanos de la Unión Europea, pero sobre este particular volveré más adelante al referirme a la normativa europea.

Los datos evidencian, señorías, que existe una creciente tendencia a la explotación de vulnerabilidades tecnológicas en productos y servicios informáticos, como sucedió con los incidentes de ciberseguridad de mayor impacto hasta el momento a nivel mundial a los que he hecho referencia, WannaCry y Petya, que aprovechan la vulnerabilidad de un sistema operativo —en este caso el conocido sistema Windows de Microsoft— para actuar. Europol estima que fueron afectados 180 países y más de 1 300 000 equipos. Qué duda cabe que una crisis de ciberseguridad de esta magnitud conlleva una alarma social que la engrandece más allá de sus consecuencias técnicas. Otra amenaza distinta proviene de la utilización del ciberespacio como medio para la realización de actividades ilícitas, incluyendo las acciones de desinformación, difusión de informaciones falsas, campañas de influencia, manipulación informativa y propaganda que, en sí mismas, como he dicho antes, no son ciberataques pero sí constituyen atentados a ese espacio seguro y fiable que pretendemos. Algunas acciones son simples pero de gran impacto, como la que sucedió en 2013, cuando un falso anuncia en la cuenta de Twitter de la agencia de noticias norteamericana Associated Press de un atentado en la Casa Blanca hizo que el Dow Jones se desplomará

cve: DSCG-12-CM-54

en pocos minutos 150 puntos. Otras son más complejas, como las actividades delictivas de redes de crimen organizado y grupos terroristas que se valen de la red oscura. Por otra parte, los servicios de inteligencia occidentales han observado un importante crecimiento del ciberespionaje económico, especialmente dirigido a industrias de los sectores de la defensa, la alta tecnología, la industria química, la energía y la salud. Además, el ciberespacio es utilizado por grupos terroristas como instrumento para realizar actividades de propaganda, comunicación interna, formación y adoctrinamiento. Hasta finales de 2015, el Ministerio del Interior de España estimaba que Daesh había difundido aproximadamente más de 1000 vídeos a través de sus cuentas de Twitter; se estima que Daesh maneja directamente alrededor de 35 000 a 70 000 cuentas. Asimismo, es cada vez más habitual el uso del ciberespacio como parte de las conocidas amenazas híbridas, que incorporan operaciones de información, subversión, presión económica y financiera junto a acciones militares, con el objetivo no solo de causar daños directos y aprovechar vulnerabilidades, sino también de desestabilizar sociedades.

Tras esta suerte de diagnóstico de la amenaza y el medio en el que operan, continuo, señorías, para tratar cómo se ha trabajado en España para cada vez más y más progresivamente incrementar los umbrales de la ciberseguridad. España no es ajena a estas amenazas, como ustedes pueden imaginar. Sin duda, en un país como el nuestro, altamente interconectado, que podríamos decir que ocupa una posición de privilegio en Europa en lo relativo al interconectado en redes y de la digitalización de nuestra sociedad, en la que existen 37 millones de usuarios de Internet, el reto de la ciberseguridad se ha afrontado desde diversas perspectivas, incluso, si me lo permiten, desde distintas culturas departamentales. Esto es así porque la ciberseguridad es una materia transversal en sí misma que afecta a todos los departamentos ministeriales de la Administración General del Estado, a todas las administraciones públicas, a la sociedad y podríamos decir que al país en su conjunto. Sin embargo, la transversalidad, como desarrollaré luego, no puede desembocar en actuaciones compartimentalizadas. En términos numéricos, según datos del Informe anual de Seguridad Nacional de 2016, presentado precisamente en esta Comisión, durante el año 2016 se registraron 106 000 incidentes de ciberseguridad en empresas, ciudadanos o infraestructuras críticas, 3,5 veces más que en el año 2015. Asimismo, las administraciones públicas hicieron frente a unos 21 000 incidentes de ciberseguridad, un 15 % más que en 2015. Según la memoria de la Fiscalía del Estado de 2017, los delitos cibernéticos más comunes son los de estafa, que sumaron 4930, lo que supone un 60 % del total. España ha apostado y sigue apostando por hacer frente a este tipo de amenazas de manera contundente. Para ello, se han ido creando las estructuras y organismos necesarios en un esfuerzo que comenzó hace dos décadas y que ha ido ganando tracción, sobre todo a partir de la creación del Consejo de Seguridad Nacional en el año 2013.

Los primeros pasos en este aspecto se remontan al año 1996, cuando las Fuerzas y Cuerpos de Seguridad del Estado empezaron a responder a las primeras denuncias de los pocos usuarios de Internet que había en aquel momento. Generalmente eran denuncias relacionadas con fraude. Estos esfuerzos culminaron con la creación de las unidades operativas especializadas, concretamente con la unidad del grupo de delitos telemáticos de la Guardia Civil y la unidad de investigación tecnológica de la Policía Nacional. Más adelante, en el año 2004, en respuesta a los rápidos avances tecnológicos, se creó, dentro del Centro Nacional de Inteligencia, el Centro Criptológico Nacional y su equipo técnico de respuesta a incidentes, el CCN-CERT, que tienen como principal responsabilidad la ciberseguridad en las administraciones públicas y el seguimiento del cumplimiento de la normativa de ciberseguridad propia de las administraciones públicas, esto es, el esquema nacional de seguridad. En el año 2006, el Ministerio de Energía, Turismo y Agenda Digital —por entonces Ministerio de Industria— impulsó la creación del Instituto Nacional de Tecnología de la Comunicación, Inteco, con sede en León, dedicado principalmente al impulso del uso de las TIC. El mundo cambia y los organismos de la Administración también se adaptan para dar respuesta al desarrollo digital y este instituto cambió de nombre para denominarse como se denomina actualmente, Instituto Nacional de Ciberseguridad, y dedicarse en exclusiva a este ámbito. En el año 2011, con el objetivo de coordinar las acciones dirigidas a proteger las infraestructuras críticas, se creó el Centro Nacional de Protección de Infraestructuras Críticas, que también acabó enfocándose en la ciberseguridad, pasando a denominarse este mismo año Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad. En el seno de este organismo también se ha creado la Oficina de Coordinación Cibernética, a fin de reforzar y centralizar todas las actividades relacionadas con la cibercriminalidad, el ciberterrorismo y la protección de las infraestructuras críticas, de manera que se puedan ofrecer respuestas eficaces y coordinadas. En nuestro compromiso con el ámbito de la ciberdefensa, en el año 2013 se creó el mando conjunto de ciberdefensa, dependiente del Jefe del Estado Mayor de la

cve: DSCG-12-CM-54

Defensa, responsable del planeamiento y ejecución de las acciones relativas a la ciberdefensa, de contribuir a dar una respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional.

Especial consideración quiero prestar, señorías, al desarrollo de nuestras capacidades en el nivel político-estratégico. Esto es así no solo por mi sesgo profesional, que distingue con claridad los planos táctico, operacional, estratégico y político como dimensiones de una respuesta óptima, integral y modular, sino porque la estructura que supone la creación del Consejo de Seguridad Nacional y el Consejo Nacional de Ciberseguridad ha propiciado entornos colaborativos para integrar las actuaciones de todos los departamentos en una suma agregada de esfuerzos. Son órganos para la cooperación reforzada que permiten tener una visión extensa y completa de todas las aristas de las cuestiones en juego. El nivel político-estratégico prioriza, dirige, coordina, fomenta las sinergias, anticipa los escenarios de evolución y decide la acción que cada actor competente en la materia debe llevar en armonía.

En suma, señorías, se trata de posicionarse en la medida de lo posible delante de los acontecimientos. Con este espíritu se crea el Consejo de Seguridad Nacional en el año 2013, una comisión delegada del Gobierno para la seguridad nacional presidida por el presidente del Gobierno, órgano imprescindible en cualquier Estado avanzado en la materia. En España, además, se han creado órganos que la apoyan en sectores de especial trascendencia en ámbitos prioritarios para la seguridad nacional como es el caso de la ciberseguridad. Me refiero al Consejo Nacional de Ciberseguridad creado en el año 2014 y que actualmente preside el secretario y director del Centro Nacional de Inteligencia. En el cumplimiento de sus funciones para mejorar la ciberseguridad en España, el Consejo Nacional de Ciberseguridad, en su reunión del 25 de febrero de 2014, adoptó un Plan nacional de ciberseguridad aprobado posteriormente por el Consejo de Seguridad Nacional. Es un avance muy importante, he de subrayarlo, ya que el plan constituye el primer nivel en la planificación de la ciberseguridad nacional y se está implementando a través de nueve planes derivados referidos a materias, entre las que me gustaría destacar tres: uno, la potenciación de capacidades; dos, potenciar el intercambio de información entre los actores implicados y, por último, potenciar la capacitación profesional en este ámbito.

También me quiero referir —entro en el tercer punto de mi exposición— a algunas cuestiones sobre la cooperación internacional como parámetro imprescindible a la hora de ordenar y proteger un espacio sin fronteras, como es el ciberespacio. Sin cooperación internacional no hay ciberseguridad posible; hay que extender los lazos de cooperación con terceros Estados, organizaciones internacionales y ampliarlos siempre de forma acorde a los principios y valores que nos explican como un Estado de derecho bien consolidado. Me centraré principalmente en el aspecto normativo de la dimensión internacional de la ciberseguridad, y lo haré porque creo que en ocasiones se decanta la balanza hacia el esfuerzo de capacidades y medios técnicos que son indudablemente necesarios, como acabo de insistir, pero se debe acompasar con nuevas reglas. España apuesta firmemente por una normativa común que conecta Estados, organizaciones y al sector privado a favor de la consecución de un ciberespacio más seguro y fiable. España es un Estado promotor y contribuidor neto a las iniciativas de desarrollo de una política de ciberseguridad coordinada en las organizaciones internacionales de las que formamos parte, fundamentalmente Naciones Unidas, OSCE y muy especialmente la Unión Europea. La colaboración en el marco de la Unión Europea es clave para nuestro país. Actualmente participamos activamente en el proceso de revisión de la Estrategia Europea de Ciberseguridad, así como en el desarrollo de la hoja de ruta para mejorar la capacidad de respuesta.

Sobre este último aspecto quisiera resaltar dos importantes procesos en los que nos encontramos inmersos: la trasposición de la directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, la conocida como directiva NIS, y la implementación del nuevo reglamento general de protección de datos de la Unión Europea. En cuanto a la directiva NIS, establece los requisitos mínimos comunes que deben cumplir todos los Estados miembros en materia de seguridad en las redes y sistemas de información, que son esenciales para el desarrollo de actividades económicas, sociales y por ende para el funcionamiento del mercado interior. En el muy avanzado borrador del anteproyecto de ley que articulará su trasposición se prevé que el Consejo de Seguridad Nacional actúe como punto de contacto único en el ámbito internacional. Podríamos decir que cuando se lleve a cabo esta trasposición España contará con la primera ley de ciberseguridad en España.

Respecto del nuevo reglamento general de protección de datos, lo que persigue es el refuerzo de la protección, el tratamiento y la libre circulación de datos personales. Se incluyen en este reglamento

cve: DSCG-12-CM-54

medidas como la obligación de comunicar las brechas o los incidentes de seguridad y realizar análisis de riesgos y evaluaciones de impacto a este tipo de incidentes. También obliga a las empresas y organismos a establecer una arquitectura de seguridad que permita una defensa apropiada de los datos que guardan. En todas estas iniciativas el papel del sector privado es fundamental, ya sea en la adopción de medidas de protección, fomento de la concienciación o desarrollo de productos y servicios de ciberseguridad. Por eso España participa activamente en la asociación público-privada sobre ciberseguridad European Cyber Security Organization, cuyo principal objetivo es apoyar todo tipo de proyectos que tengan como fin desarrollar, promover y fomentar la ciberseguridad en la Unión Europea.

Podríamos decir que España se encuentra en el vagón de cabeza a nivel internacional de la ciberseguridad. Según el *ranking* de la ciberseguridad elaborado por la Unión Internacional de Telecomunicaciones, conocida como OIT —organismo perteneciente a Naciones Unidas—, nos encontramos en el puesto 19.º a nivel mundial entre 193 países evaluados. Nos encontramos por delante de países como Brasil, Argentina o Colombia. A nivel de la Unión Europea nos situamos en un 7.º puesto, teniendo por delante a Estonia, Francia, Reino Unido, Holanda, Finlandia y Suecia, y por detrás a países como Alemania, Italia, Dinamarca y Portugal.

Abordo ya, señorías, el cuarto y último punto de mi intervención donde, como les mencioné, quiero compartir tres cuestiones que para nosotros, para el Departamento de Seguridad Nacional, son importantes de cara a fortalecer la prevención, detección, respuesta y, a la postre, resiliencia frente a los ciberataques. Estos tres puntos son la gestión de crisis, la cultura de ciberseguridad y la cooperación privada. En cuanto a la gestión de crisis, en la era de la conectividad, de la expansión del ciberespacio, cualquier tipo de incidente de ciberseguridad por pequeño que sea puede llegar a tener grandes repercusiones. Un incidente técnico de cualquier tipo, ya sea un ciberataque o un mal uso de la tecnología, puede llegar a originar una crisis con efectos sobre el normal funcionamiento del país, incluyendo la economía, los servicios esenciales, la salud, el agua, la energía o el transporte. Podría incluso impactar negativamente en la reputación de cualquier organización, ya sea pública o privada, o mermar los sistemas y los medios de comunicación pública. Aunque pudiera parecer que este tipo de incidentes solo requieren de una respuesta técnica para frenar la infección y recuperar los sistemas informáticos, sus efectos demandan respuestas mucho más amplias e integrales que se mueven en los tres niveles a los que hice alusión —táctico, operativo, estratégico o político-estratégico— y precisan la colaboración internacional, el refuerzo y la coordinación nacional entre distintos sectores, en donde se incluyen el legislativo, el judicial, la comunicación, para asegurar la gestión. En este sentido, el modelo de gestión de crisis en el marco del sistema de seguridad nacional ha avanzado significativamente. El Departamento de Seguridad Nacional es el órgano de la Presidencia del Gobierno que comunica las labores técnicas de los Certsi, los centros de respuesta ante incidentes de ciberseguridad, con las decisiones estratégicas del Consejo Nacional de Ciberseguridad y el Comité de Situación, órgano este último que asiste al Consejo de Seguridad Nacional en materia de gestión de crisis. Es un comité de carácter único que se apoya en el centro de situación del Departamento de Seguridad Nacional.

En aras de la anticipación, la prevención, y porque en definitiva se juega como se entrena, en las crisis, cualquier pérdida de tiempo es intolerable. Se deben procedimentar, practicar y ejercitar. Además de contar con las estructuras y herramientas necesarias para la gestión de crisis, es importante aplicarlas a través de la participación en ejercicios y simulacros de ciberseguridad, como se hace en el ejercicio de gestión de crisis de la OTA o en el Cyber Europe, el mayor ejercicio a nivel organizado por la Unión Europea, en el cual el Departamento de Seguridad Nacional coordina la participación nacional tanto de los organismos públicos como de actores privados que participan.

Por lo que se refiere a la cultura de la ciberseguridad, lo primero que hay que decir es que nadie es un consumidor pasivo de seguridad. La hiperconectividad y el desarrollo tecnológico, a los que me he referido extensamente durante mi intervención, unidos al crecimiento del número de usuarios, hacen inevitable la exposición a amenazas en el espacio donde interactuamos. Es esencial desarrollar una cultura de ciberseguridad que nos haga más resilientes como sociedad, fomentando la concienciación sobre el uso seguro de la tecnología y la importancia de nuestra privacidad en la Red. Si bien la seguridad absoluta no existe, casos relacionados con el cibercrimen, como el robo de datos, de números de tarjetas de crédito, la extorsión o el acoso, demuestran que la concienciación sobre las amenazas existentes y la adopción de medidas de autoprotección redundarán en la disminución de nuestra vulnerabilidad. En 2015, el Consejo Nacional de Ciberseguridad desarrolló el Plan nacional de cultura de ciberseguridad, uno de los nuevos planes a los que me he referido y que fueron aprobados posteriormente por el Consejo de

cve: DSCG-12-CM-54

Seguridad Nacional. Este plan desarrolla proyectos concretos en este sentido que ya se están ejecutando. Por citar algunos, la participación de España en el Mes Europeo de la Ciberseguridad, organizado por Enisa; el trabajo del Centro Criptológico Nacional, creando una estrategia de generación de información que sirva de concienciación a las administraciones públicas; la puesta en marcha del Centro de Seguridad en Internet para menores de edad, cuyo objetivo es la promoción del uso seguro y responsable de Internet; y las nuevas tecnologías entre niños y adolescentes. La futura estrategia de Seguridad Nacional del año 2017 contempla como uno de sus objetivos principales la promoción de la cultura de seguridad nacional para impulsar actuaciones como las que he mencionado anteriormente.

En último lugar, en cuanto a la colaboración público-privada, el intercambio de información y de inteligencia entre el sector público y privado es un factor clave en la lucha contra las ciberamenazas, ya que proporciona una visión mucho más completa del mapa de ciberseguridad y de las vulnerabilidades existentes. Por este motivo, el modelo integrado de gobernanza que ha desarrollado España contempla la colaboración del sector privado en las iniciativas de seguridad nacional, desde el desarrollo de las políticas de ciberseguridad nacional hasta la gestión de crisis y el aseguramiento de la continuidad de los servicios. Hay que recordar que más del 80 % de los servicios esenciales en España están en manos del sector privado. La cultura de ciberseguridad ha de llegar al sector privado, denominación bajo la cual hay tres actores muy diversos; y el desarrollo de un mercado nacional de ciberseguridad fuerte y competitivo es también un objetivo compartido.

Se están realizando grandes esfuerzos para fomentar la inversión en ciberseguridad, que requiere y exige una gran aportación del sector privado. Algunas de las iniciativas existentes son: el programa de emprendimiento en ciberseguridad, *Cybersecurity Ventures;* el programa de aceleración de *startup* en ciberseguridad; o las misiones comerciales internacionales para presentar la oferta española en ciberseguridad; estas últimas en colaboración con el Instituto Español de Comercio Exterior, el ICEX. Sin embargo, señorías, hay margen sustantivo de mejora, principalmente en lo que se refiere al aumento de confianza entre el sector público y el sector privado, en la apuesta por el I+D+i o la capacitación y formación de profesionales en materia de ciberseguridad. Precisamente uno de los problemas a los que nos enfrentamos es la falta de profesionales cualificados en la materia. La Comisión Europea estima que la demanda de empleos con cualificaciones digitales crece en torno a un 4 % anual, y que el déficit de profesionales especialistas en el sector tecnológico, de aquí al año 2020, podría alcanzar los 825 000 empleos vacantes dentro de la Unión Europea. La escasez de profesionales de las TIC no es exclusiva en términos de capacidades técnicas, sino que cada vez hay más demanda de perfiles relacionados con la gestión, la auditoría y el cumplimiento normativo en materia de ciberseguridad.

En el estudio realizado por el Instituto Nacional de Ciberseguridad, denominado *Punto de partida al modelo de gestión y seguimiento del talento en ciberseguridad en España*, se refleja la necesidad de seguir dirigiendo nuestros esfuerzos a la generación, detección, identificación, retención y gestión del talento a través de las medidas concretas, como la educación temprana en esta materia; una mejor formación que dará respuesta a la oferta de empleo en este ámbito, especialmente en la formación de profesionales; la sensibilización de las empresas sobre el valor del profesional de la ciberseguridad; o la organización de eventos para identificar y captar talentos en ciberseguridad.

Señorías, quiero concluir reiterándoles el honor que supone para mí comparecer hoy en esta Cámara, y quedo a su disposición para los comentarios o preguntas que me quieran formular.

Muchas gracias por su atención.

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

Vamos a abrir un primer turno de intervenciones. Si les parece, el primer turno será de diez minutos de intervención. En primer lugar, por el Grupo Mixto, tiene la palabra el señor Yanguas.

El señor **YANGUAS FERNÁNDEZ:** Muchas gracias, señor presidente.

Voy a intervenir brevemente, en primer lugar, para agradecer al director operativo de Seguridad Nacional, señor Castellón, por estas explicaciones que nos acaba de dar aquí esta tarde. Quiero destacar algunos datos que he podido ver, desde el desconocimiento que yo tenía, y que he podido recabar a día de hoy con lo que acabamos de escuchar. Desde luego sobre la multiplicación de los ciberataques —usted lo ha comentado en varias ocasiones durante su intervención— es importante conocer que están aumentando de manera exponencial, y por tanto es necesario defenderse cada vez más y mejor. En segundo lugar, sobre la falta de datos sobre los ciberataques, usted ha hablado, incluso en la memoria del año pasado, de un número de ataques que ha habido, pero yo me pregunto, ¿están todos los que son

cve: DSCG-12-CM-54

ahí en esa memoria? Porque si desconocemos que ese ciberataque se ha dado y su alcance poco podemos hacer para intentar evitarlo la próxima vez. Usted también ha hecho referencia en su intervención a que en la próxima ley o en el reglamento de protección de datos será obligatorio para las empresas y para las entidades comunicarlo; así, si lo sabemos o si el Gobierno lo sabe nos podremos defender desde luego mejor.

Yo había apuntado también —y usted ha hecho referencia ahora mismo a ello al final de su intervención— la falta de personal cualificado en ciberseguridad. Es bien conocido que en este aspecto de la tecnología, que va avanzando a pasos agigantados, hace falta personal cualificado. Además usted nos ha hablado de dos cosas: de iniciativas público-privadas y también de algún dato concreto para mejorar la capacitación de esos profesionales. Yo le quería preguntar si usted es optimista con este tema y si vamos a ir a mejor si hay más profesionales que se dediquen a esto.

También le quería preguntar si hay algún *ranking* sobre ciberseguridad, cuestión que usted ya me ha respondido diciendo que estábamos en el puesto diecinueve del mundo y en el séptimo de Europa, lo que desde mi desconocimiento creo que está muy bien, pero entonces me viene a la cabeza otra pregunta, y es si estamos evolucionando a mejor, si iremos a mejor en esos *rankings,* según su experiencia, o si cree que los demás países están corriendo más en este materia porque están invirtiendo más o por lo que quiera que sea. Me gustaría conocer su opinión al respecto.

Y dentro de España desconozco cuál es la dinámica entre las comunidades autónomas y la Comunidad Foral de Navarra, de la que yo provengo, y si hay algún tipo de coordinación en este tema concreto de la ciberseguridad, cuestión sobre lo que no le he escuchado nada, por lo que me gustaría que me dijera algo, si es que eso existe a día de hoy.

Muchas gracias; buenas tardes.

El señor **PRESIDENTE:** Muchísimas gracias, señor Yanguas.

Tiene ahora la palabra el señor Legarda.

El señor **LEGARDA URIARTE:** Muchas gracias, presidente, y muchas gracias también al compareciente por la charla tan ilustrativa que nos ha dado.

Yo quisiera hacer un par de preguntas simplemente referidas a la seguridad en sí misma considerada, no como instrumento. Usted no lo ha dicho, pero se deduce claramente de sus palabras que esta cuestión constituye una amenaza vital en los términos de la Ley de Seguridad Nacional. Otra de las características que tiene es su manifestación proteica: afecta a todas las realidades, a todos los niveles, de manera transversal. En este sentido también ha manifestado usted que una de las claves es el trabajo en red y la suma agregada de fuerzas o capacidades que protejan de manipulaciones y que garanticen la no alteración de medios tecnológicos.

Yendo a las preguntas en este contexto, usted ha tratado de aquellos avances que se han ido produciendo en el ámbito del Estado; no ha citado a las comunidades autónomas, pero obviamente esa es una realidad transversal de la cual tiene que dotarse cualquier operador privado y entiendo que cualquier Administración pública. En este sentido ha dado un salto y ha hablado del nivel regional europeo, en dos aspectos: protección de datos y medidas mínimas. Teniendo en cuenta las características que usted ha definido de esta ciberseguridad en sí misma, considerada proteica, en red, suma de capacidades, ¿qué medidas se están tomando o qué grado de relación tiene nuestro nivel regional más inmediato, de Europa, con otros niveles regionales internacionales? Porque finalmente Europa no deja de ser, a efectos de ciberseguridad, una realidad desconectada y su clave es el trabajo en red, la suma de capacidades a nivel global, porque estamos hablando de una amenaza vital concreta para nosotros, pero también de una amenaza global.

En Europa ya vemos que tenemos grandes divergencias en protección de datos respecto al bloque americano. Ahora mismo, respecto a los reglamentos que se están trasponiendo, tenemos grandes problemas a la hora de leernos con la protección de datos del bloque norteamericano, pero también está el bloque asiático-pacífico, etcétera. Con relación a ellos estamos en mantillas. Estamos hablando de un sumatorio regional, pero eso evidentemente no es suficiente, y las medidas mínimas lo son en cuanto a un estándar europeo. ¿Hay un estándar internacional de medidas mínimas? El nivel europeo es un avance, pero la amenaza es global y la protección es regional, que sería lo mismo que estatal, por tanto la pregunta es cómo se está trabajando en este sumatorio agregado de capacidades a nivel mundial, porque la amenaza es global.

cve: DSCG-12-CM-54

Voy acabando. La segunda pregunta es: ¿entiende usted que en este momento, teniendo en cuenta esta amenaza de la ciberseguridad en sí misma considerada, lo cual supone la afectación a medios tecnológicos, esta puede afectar a procesos electorales desde el punto de vista del voto electrónico? La modernidad es una cuestión que está encima de la mesa, pero a su vez existe la amenaza de la posible manipulación. Países que tenían instalado este sistema parece que son renuentes respecto a ciertas aplicaciones. No sé ahora mismo si ha sido Holanda o algún país báltico el que se está cuestionando esto. Me gustaría saber su opinión respecto a la implantación del voto electrónico. Se está manejando incluso en esta Cámara como una alternativa, no formalmente, pero hay propuestas para el famoso voto CERA de los españoles residentes en el extranjero como una medida de agilizarlo, porque la mecánica es compleja. Quisiera conocer su opinión concreta y si es recomendable en este momento o hay medidas suficientes para gestionar un proceso político a través de voto electrónico con las amenazas que conocemos.

Muchas gracias.

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

Tiene ahora la palabra el señor Gutiérrez.

El señor **GUTIÉRREZ VIVAS:** Muchas gracias, señor presidente.

Muchas gracias, señor Castellón; creo que su exposición ha sido muy reveladora, pero también muy bien documentada; ha contado todo lo que se ha hecho y lo que se está haciendo, que creo que es bueno, pero insuficiente. Me temo que debo juzgar su comparecencia como optimista. El mundo de la realidad, sobre todo el mundo de la realidad de nuestras empresas es al final un mundo importante en cuanto a que son los principales amenazados, y por tanto parte de la amenaza que afecta al resto. Ahí tenemos las redes de *bots* que pueden acabar inundando todo nuestro ecosistema de pequeñas y medianas empresas, de pymes, que están muy alejadas de los estándares de seguridad internacionales y nacionales.

Voy a intentar ordenar un poco lo que le quiero comentar, porque hay varias cosas que creo que son importantes y en las que me da la sensación de que el Estado —el Gobierno en este caso— no está trabajando adecuadamente. Uno tiene que ver con la concienciación a nuestras empresas de lo importante que es la ciberseguridad. En España parece que lo del todo gratis se ha impuesto y se impuso durante mucho tiempo, en un mundo en el que España ha sido pionera en la piratería de muchísimas cosas; piratería en el acceso a la cultura, pero también en el acceso a los programas informáticos, en el consumo. Aquí nadie pagaba un antivirus, nadie pagaba un *software* oficial, todo se pirateaba, se bajaba de Internet. Esta cultura existe y cala; ha calado en nuestros jóvenes desde los colegios. No hay formación adecuada en ciberseguridad porque no hay formación adecuada en el respeto a lo importante que es la protección del *software* como un activo, y por tanto también como un activo de protección a la seguridad. Creo que no hay una formación adecuada; desde las escuelas no se fomenta una formación adecuada por parte del Ministerio de Educación, pero tampoco desde el Ministerio de Industria una formación adecuada a nuestras empresas sobre cuál debe ser la inversión. La seguridad es cara y esto es así, hay que entenderlo, es cara en todo caso; la ciberseguridad también. Todos sabemos que montar una alarma en tu casa cuesta más que no tenerla; que montar tres cerrojos en tu casa cuesta más que tener uno. También en una empresa montar los *firewall* adecuados, los sistemas de protección adecuados acaba siendo más costoso. Pero es necesario invertir ahí porque no solo protege tu empresa, protege al entorno de tus clientes y al final, como no puede ser de otra manera en un entorno colaborativo, acaba protegiéndonos a todos. Creo que se está trabajando poco en esto y es una cuestión sobre la que me gustaría saber qué opina, aunque creo que la Administración tiene que hacer un enfoque grande.

Le voy a poner unos ejemplos. Usted nos hablaba ahora mismo de la Directiva NIS, que es una directiva europea y evidentemente internacional para la Administración. La ISO 27001 existe desde hace muchísimos años, no hay ninguna Administración en España, ningún ministerio que esté certificado en ISO 27001, ninguno. Si nuestra propia Administración no se certifica en los estándares de seguridad internacionales, si cuando contrata servicios no exige en los pliegos de condiciones que las empresas —porque solo se contrata sobre la base del precio— estén certificadas en seguridad —las empresas que son contratistas de la propia Administración— es difícil que la seguridad, que es algo que debe de calar como una especie de lluvia fina, acabe calando en el concepto de nuestras empresas. Creo que la administración tiene una responsabilidad muy importante a la hora de hacer que nuestras empresas están certificadas. Le he hablado de la 27001. No le quiero decir nada de la PCI DSS, otra certificación específica para tarjetas de crédito en la que toda la Administración —hay mucha parte de la

cve: DSCG-12-CM-54

Administración, sobre todo en Hacienda y Seguridad Social— que trabaja con tarjeta de crédito no está certificada en PCI DSS. Eso significa que los datos de las tarjetas de crédito de los ciudadanos no están protegidos. Yo creo que es algo en lo que debe trabajar. Hay otros estándares más, el IPA, otro estándar americano. Tampoco. Ningún estándar se está utilizando en la Administración ni tampoco se obliga a que cuando se contrata con la Administración las empresas contratistas tengan este tipo de estándares, lo cual hace que no haya cultura de la ciberseguridad. No hay campañas oficiales, no hay campañas de publicidad institucional sobre ciberseguridad, y eso hace que al final, unido a este fenómeno perverso que yo decía de que aquí todo es gratis, nos encanta la piratería y bajarnos del eMule todas las cosas, al final esto no acaba de desarrollarse.

Creo que también hacen falta juzgados específicos en el delito de la ciberseguridad. No tenemos. Me parece que nuestra Administración de Justicia en este caso necesita que haya formación adecuada, tanto en la fiscalía como en los juzgados de primera instancia e instrucción sobre especialización en un tema que evidentemente es complejo para los jueces y para los fiscales. Yo creo que es necesario que se trabaje mucho en este sentido.

Le daba antes un ejemplo del mal uso por la propia Administración de estos estándares. Ahí tiene usted Lexnet. No me quiero extender en el caos de Lexnet. Si queremos tener lo opuesto a un software seguro ese es Lexnet, con unos agujeros tremebundos, y esto lo ha contratado la Administración. No hay definición de estándares de seguridad ni tampoco de control de lo que se está haciendo. Por eso digo que creo que su presentación es fantástica, pero que en este sentido es un poco optimista.

Sobre el tema de la Ley de Protección de Datos le diría que estamos en una trasposición de esta nueva directiva europea que creo que está bastante bien, por lo que vamos conociendo los grupos parlamentarios, pero me extraña que la propia Administración no esté trabajando en la actualización de la acreditación de *safe harbor* por parte de Estados Unidos a la hora de transferir datos y a la hora de comunicar datos personales con empresas que están en Estados Unidos. Tenemos que pensar que en España hay muchísimas multinacionales y los datos de los empleados nacionales acaban en servidores americanos. Yo creo que la directiva sobre *safe harbor,* que se cerró entre la Unión Europea y el Gobierno americano hace casi quince años ha quedado obsoleta frente a estas amenazas. Creo que la Administración debería trabajar más en que este protocolo *safe harbor* fuera mucho más exigente y se adecuara más a la nueva regulación que viene de Europa en la trasposición de esta directiva. Creo que tenemos un doble reto, como decía antes, el doble reto cultural, que para mí es muy importante, y el reto de que la Administración se adecue tecnológicamente, porque al final debe ser esa especie de máquina tractora que acabe arrastrando detrás de sí no solo al resto de la Administración, en este caso autonómicas o locales, sino también a toda la empresa privada que trabaja con ella.

Finalmente, para acabar, respecto al tema de la formación, creo que tenemos una oportunidad tremenda en este país de formar a los profesionales en algo que ya es una realidad y una necesidad hoy en día, pero que lo va ser muchísimo más en los próximos años. Creo que el nuevo modelo de educación, pensar que la educación no solamente consiste en sacar una certificación más en una universidad o una titulación más en una universidad o en otra, sino que tiene que ser algo que parta de la base de cambiar el concepto en la base de cómo hacemos la educación, de no educar tanto en la repetición, en la memoria, sino educar en la lógica, en el pensamiento, en el discurso, en el desarrollo, va a ayudar muchísimo más a que nuestros jóvenes y nuestros menores hoy en día acaben convirtiéndose en grandes profesionales de algo que evidentemente va a ser muy demandado.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Hay que ver lo que sabe usted, señor Gutiérrez.

Señor Comorera, tiene la palabra.

El señor **COMORERA ESTARELLAS:** Muchas gracias, señor presidente.

Lo primero es agradecer, cómo no, la presencia hoy aquí y las explicaciones que nos ha dado el señor Castellón, que a los que somos legos en temas de ciberseguridad nos parecen muy interesantes. Voy a insistir en los mismos términos que los compañeros que me han precedido en el uso de la palabra, pues básicamente mis preguntas son muy parecidas a las que ha hecho el portavoz de Ciudadanos. El supervisor europeo de protección de datos alerta sobre las deficiencias de la estrategia de la Unión Europea en materia de protección de datos, y llama la atención para que la seguridad informática no se convierta en una excusa para controlar ilimitadamente la información personal de los ciudadanos. A este

cve: DSCG-12-CM-54

respecto me gustaría que me aclarara cómo se puede hacer partícipe de esta estructura, tanto al sector privado como a la ciudadanía, en el contexto de esta estrategia garantizando la salvaguarda de los derechos fundamentales de nuestra Constitución.

En cuanto al alcance que supone hoy la utilización de las redes en el ámbito social, al hilo de la ciberseguridad, teniendo en cuenta, según los datos que nos ha facilitado, que el delito número uno es el ciberdelito, ¿cree que es necesario aumentar la formación en las nuevas tecnologías, en el desarrollo de las mismas a las Fuerzas y Cuerpos de Seguridad del Estado: capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad? Más que juzgados especializados, como comentaba el portavoz de Ciudadanos, teniendo en cuenta, según los números que aparecen en la memoria de la fiscalía, el aumento de los delitos relacionados con la ciberseguridad, tendríamos que especializar a todos los juzgados, pues de cara al futuro es posible que la mayor parte de los delitos estén relacionados con la ciberseguridad. Quizá esa especialización tendría que ser más general de toda la sociedad, incluyendo a las Fuerzas y Cuerpos de Seguridad del Estado, al ejército y, cómo no, a los juzgados, a las fiscalías, etcétera, más que unos juzgados especializados. Me gustaría conocer su opinión al respecto.

Al igual que ha manifestado el portavoz del Partido Nacionalista Vasco, ¿cómo se garantiza la no injerencia de terceros Estados y de qué medios disponemos para que no ocurran en España hechos como los denunciados en Estados Unidos durante su proceso electoral, como lo que ha pasado recientemente en Francia, donde se denunciaban los mismos hechos, o el presunto reciente que da cuenta a la prensa de unos *hackers* rusos en Cataluña?

Me gustaría saber si cree que tenemos que tomar algún tipo de medida legislativa que no exista a día de hoy en nuestra legislación para luchar contra los delitos de ciberseguridad, teniendo en cuenta la enorme dificultad por el avance continuo de este tipo de amenazas. El trámite legislativo de cualquier reforma siempre va mucho más lento, y cuando llegamos a la ley, ya está superada por nuevos problemas. Quisiera conocer su opinión.

Para finalizar, como señalaba el portavoz de Ciudadanos, yo tampoco soy muy optimista al respecto. Hoy he leído que la auditora Deloitte —la noticia ha salido en *The Guardian*— ha sufrido un *hackeo* masivo. Deloitte es una de las consultoras preferentes de Incibe, una de las mayores consultoras de ciberseguridad española por el número de contratos que tiene con Incibe y ha sufrido un *hackeo* que ha puesto al descubierto cuentas de clientes, contraseñas, correos e información de carácter personal. Esto me asusta. Si una de las compañías que más nos asesora en esto es *hackeada*, lógicamente lo vemos como un problema y me gustaría conocer su opinión.

Muchas gracias.

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

Tiene la palabra el señor Hernando.

El señor **HERNANDO VERA:** Gracias, señor presidente. Gracias también al señor Castellón por su comparecencia y por su exposición.

Mi grupo coincide con la preocupación, la importancia y el interés que el señor Castellón ha manifestado que tiene el Gobierno en esta materia de ciberseguridad. Un ejemplo es la evolución, tanto legislativa como operativa, que se ha producido en los últimos años, especialmente a partir de 2012 o 2013 con la estrategia nacional o la propia aprobación de la ley que ha dado lugar a la creación de esta Comisión. Pero creo que todos vamos a coincidir —seguramente también el señor Castellón— en que tenemos que ir más rápido y ser más ambiciosos. Hemos hecho cosas, pero esto va tan rápido que muchas veces cuando llegamos ya lo hacemos tarde, porque seguramente deberíamos tener más medios. Esa es una de las cosas a las que no se ha referido el señor Castellón. ¿Son los medios suficientes? La Estrategia de Seguridad Nacional se empezó a montar objetivamente en España en un tiempo de crisis económica, y por lo tanto los recursos en un tiempo de crisis económica para una estrategia de la importancia y el coste que tiene esta seguramente no fueron suficientes entonces y seguramente no son suficientes tampoco ahora. Imagino que a todas las agencias encargadas de esto les gustaría en estos momentos tener más recursos. Por otra parte, hay que asignar esos recursos a las ciberamenazas que se producen, y no todas las ciberamenazas son de la misma intensidad e importancia, y por lo tanto no sé si se ha hecho una asignación de recursos por tipo de amenaza o de ciberamenaza.

¿Estamos bien en España? Estamos bien, pero no excelentemente, como han dicho ya otros intervinientes. Nos ha dado el índice mundial de ciberseguridad. No sé a qué año se refería. Yo tenía unos

cve: DSCG-12-CM-54

datos de 2015 según los que estábamos en el grupo nueve, puesto numérico treinta y tres. Si no recuerdo mal, nos ha dicho que estamos en el puesto numérico diecinueve, por delante de algunos países, pero por detrás de otros. Tenía entendido que algunos países latinoamericanos como Colombia, Brasil o Uruguay estaban por delante de nosotros. Si ha mejorado eso en dos años es que hemos hecho muchas cosas, pero seguramente tenemos que hacer muchas más. En todo caso conocerá el informe de Microsoft de inteligencia sobre seguridad global que señala a España con una afectación por *malware* del 23 %, mientras la media mundial está en el 20 %; fundamentalmente *malware* consistente en troyanos en el 23 % de los ordenadores en España. Por tanto es muy necesaria la concienciación y la autoprotección de las que ha hablado en algún momento el señor Castellón.

Trasposición de la directiva. Deduzco de sus palabras que, si el anteproyecto está muy adelantado y avanzado, va estar antes del 9 de mayo de 2018, que es el plazo máximo de trasposición. Eso será importante, pero nos ha anunciado que va a haber un nuevo punto nodal de relación con el resto de autoridades europeas y mundiales. Eso modifica lo que se ha aprobado este verano mediante el Real Decreto 770/2017, que establece como punto de contacto la Oficina de Coordinación Cibernética. Este real decreto —le refresco la memoria— es el que establece la estructura orgánica básica del Ministerio del Interior, da competencias en esto a la Secretaría de Estado de Seguridad y crea el Centro Nacional de Protección de Infraestructuras y Ciberseguridad, dentro de la secretaría de Estado. Lo único que quiero saber es si esto lo modifica o no lo modifica. Quiero que nos aclare si la trasposición de la directiva va a suponer una modificación de la asignación, como punto de contacto nacional, a la Oficina de Coordinación Cibernética, que depende del Centro Nacional de Protección de Infraestructuras y Ciberseguridad.

Nos ha hablado el señor Castellón de las distintas culturas departamentales, cosa que es importante. Eso puede ser enriquecedor, pero también puede ser un desastre. Seguramente uno de nuestros principales problemas es el autopatrón de protección, sobre todo cuando hay un patrón de protección distinto, dependiendo de las distintas administraciones, de los distintos departamentos dentro de las distintas administraciones, y no le digo ya entre el sector público y el sector privado. Ahí tenemos un problema. Precisamente una estrategia nacional de ciberseguridad tiene que intentar establecer un patrón único que sirva de modelo. Yo creo que ahí tendremos que trabajar mucho más para que no haya eso que ha llamado distintas culturas departamentales, porque las distintas culturas departamentales seguramente no son beneficiosas a estos efectos.

Nos ha hablado de la industria de la ciberseguridad y del potencial que tiene esta industria, de la escasez de medios humanos especializados, y en este tema tenemos que hacer mucho más porque tenemos duros competidores dentro de la propia Unión Europea. Está Francia exportando su marca Francia de ciberseguridad, muy apoyada por sus autoridades y por el Ministerio de Exteriores, pero también está el Reino Unido que, a través de su diplomacia económica, tenía el objetivo de exportar 2 billones de libras en servicios de ciberseguridad y en material de ciberseguridad. Ahí necesitamos mucho más impulso del Gobierno y de la Administración central, incluso más implicación también del Ministerio de Exteriores. Nos ha hablado del ICEX y de su programa, y creo que ahí tenemos una grandísima ventana de oportunidad para España, para la industria española y para los profesionales españoles que se están especializando en este tema.

Voy al último punto que quería tratar y que me ha interesado especialmente, que son algunos agentes de amenaza, algunas amenazas concretas en función de los agentes. Que los ciberdelincuentes hagan ciberataques es hasta cierto punto razonable, los delincuentes se dedican a atacar; pero cuando esa ciberdelincuencia se produce por parte de agentes estatales, entonces el problema es más grande o tiene otra dimensión. Lo que quiero preguntarle es si se han detectado agentes estatales detrás de determinados ciberataques que se han conocido en los últimos tiempos. Sabemos que hay una Comisión del Congreso de los Estados Unidos que está investigando los ciberataques a la campaña de una de las candidatas, de la señora Clinton, en las últimas elecciones norteamericanas. Sabemos que hay auténticas actuaciones de *hacking* político, *hacking* político en la red, porque el *hacking* político en general siempre ha existido; quiero decir que el espionaje político siempre ha existido. Watergate es espionaje político. Lo que pasa es que ahora se produce a través de la red y ahora se produce con intención de influir en la opinión pública y de trasladar noticias falsas que se convierten en virales y que influyen en los procesos electorales o en los procesos políticos.

Aquí se ha mencionado ahora mismo por parte del portavoz que me antecedido en el uso de la palabra, que ha habido un periódico de ámbito nacional que ha titulado a toda portada, en cuatro columnas, el pasado 23 de septiembre: La maquinaria de injerencia rusa penetra en la crisis catalana. **(Muestra una**

cve: DSCG-12-CM-54

fotocopia de un periódico). Simplemente leo el titular. Lo que quiero saber es si en el observatorio que usted tiene en la Secretaría Técnica del Consejo de Seguridad Nacional o a través del asesoramiento del presidente del Gobierno en esta materia hay información sobre esto; y si no la hay, cuáles son los medios que se están poniendo para conocer si esto es así o no es así, no ya para hacer algo o no, porque, como usted nos ha dicho, el problema es la trazabilidad y las dificultades para conocer la autoría última de todas estas cuestiones.

Muchísimas gracias por su exposición.

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

Para terminar este turno de intervenciones, tiene la palabra la señora Vázquez.

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

En nombre del Grupo Parlamentario Popular, agradecemos la comparecencia del señor Castellón. Ha sido una comparecencia extensa y muy interesante. De las veinte preguntas que le quería formular el Grupo Popular, diez ya las ha contestado en su exposición.

Comenzaba diciendo que la tecnología avanzaba, y eso hace que también nosotros tengamos que ir modificando la normativa a medida que la tecnología avanza. Estamos hablando de que no conocemos, de que no existe un titular virtual, con lo cual estos ciberataques muchas veces se esconden bajo el anonimato y, lógicamente, es un desafío constante al que se están sometiendo los países. Felicitamos a todo el personal, en concreto al Departamento de Seguridad Nacional, por el *ranking* que ocupamos. Desconocía que estábamos tan bien situados. Considero que en un *ranking* a nivel mundial el puesto 19 es un puesto bueno, y a nivel europeo el 7 también lo es, aunque podemos mejorarlo; efectivamente, coincidimos en eso.

Le voy a hacer algunas preguntas. ¿Se ha diseñado alguna política orientada —creo que usted aquí habló de ello— a la detección temprana de talento en materia de ciber? ¿Hay alguna estrategia para preparar a jóvenes en edades preuniversitarias? ¿Considera que existen suficientes recursos de talento en materia ciber, dentro de las estructuras de ciberdefensa y ciberseguridad, para afrontar una situación de crisis?

Usted también mencionaba que en un futuro iban a faltar profesionales. ¿Ha considerado la posibilidad de disponer de una reserva estratégica de talento, de una ciberreserva o grupo de reservistas en materia de talento para ciberataques y respuestas a ciberataques masivos? ¿Cree que las estructuras de cooperación público-privadas se encuentran bien diseñadas para hacer frente a un ataque contra una o varias infraestructuras críticas? ¿Considera que, sobre la base de la interrelación entre los ámbitos de ciberseguridad y ciberdefensa, las relaciones de cooperación entre los organismos adscritos a cada uno de los perímetros de defensa son los adecuados en estos momentos? ¿Qué valoración nos podría hacer usted de los resultados de esa cooperación?

Esta cuestión también se ha mencionado aquí en varias ocasiones, pero le pregunto: ¿Ha realizado su departamento estudios de impacto sobre nuestro país de posibles injerencias haciendo uso de técnicas y tecnologías avanzadas de influencia por parte de cualquier actor en el ciberespacio? Por actor entiéndase Estados y entiéndase privados. En caso de no existir, ¿se tiene prevista la creación de un departamento de detección de campañas de influencia y generación de inteligencia contraargumental? Creo que Estados Unidos está estudiando ahora esa posibilidad. Esto viene a raíz de lo que hemos conocido sobre Cataluña, de la red global, que Rusia ha actuado en campañas a favor de Trump o del *brexit.* ¿Le consta al Departamento de Seguridad Nacional que se está haciendo algún tipo de campaña para influenciar en el tema de Cataluña? ¿Aparte de esta campaña, que conocíamos por los medios de comunicación rusos, hubo intentos de hacer más campañas de influencia o le consta que algún Estado pueda estar detrás, si es que ha existido?

Le iba a preguntar por las relaciones de cooperación con el sector privado. Nosotros estamos a favor de incrementarlas y potenciarlas, y va a contar con el Grupo Parlamentario Popular para cualquier modificación que haya que hacer al respecto.

Por último, ¿cómo afectará a España la creación de la Agencia Europea de Ciberseguridad propuesta por el presidente de la Comisión Europea y que anunció hace escasamente unos días?

Por lo demás, desde nuestro grupo parlamentario queremos felicitarle por el trabajo que están haciendo. Sabemos que el desafío es contante y diario. Hace meses, cuando sufrimos, al igual que esos 180 países, ese ciberataque masivo, España respondió de una manera contundente y desde el

cve: DSCG-12-CM-54

Grupo Popular tenemos que felicitar a toda la gente que colaboró ese día para que no sufriéramos daños mayores en los servidores.

Muchas gracias.

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

Señor Castellón.

El señor **DIRECTOR OPERATIVO DEL DEPARTAMENTO DE SEGURIDAD NACIONAL** (Castellón Moreno): Muchísimas gracias, señor presidente.

En primer lugar, todas las preguntas o comentarios son muy acertados y tienen delimitado perfectamente el problema, el impacto y las consecuencias. Son preguntas y observaciones muy acertadas sobre el estado de la ciberseguridad en España. Voy a tratar de matizar algunas de las preguntas que me han formulado.

En primer lugar, contestando a las preguntas del señor Yanguas, del Grupo Mixto, se suele decir que hay dos tipos de empresas: las que han sufrido un ciberataque y las que no se han dado cuenta de que lo han sufrido; prácticamente todas las empresas han sufrido un ciberataque y muchos no se han detectado. Ligándolo con las estadísticas, ¿por qué también, entre otras cosas, crece el número de incidentes? Porque empezamos a darnos cuenta de lo que pasa y hace años no sabíamos nada al respecto; ahora empezamos a detectar los incidentes y empezamos a ver que aumentan. Es verdad que aumenta el número de ataques, pero también es verdad que nuestras medidas para detectarlos se han incrementado de una forma tremenda en los últimos años. España, junto con los países de nuestro entorno, hemos empezado a actuar de una forma decidida en materia de ciberseguridad hace muy pocos años. Hablamos del año 1996, cuando se crea en la Guardia Civil y en la Policía una unidad de delitos telemáticos; en 2004, el CNI crea un centro criptológico que acaba convertido en una unidad de ciberseguridad. Es decir, tanto nosotros como los países de nuestro entorno llevamos quizá diez años lidiando con este problema, no más.

Contestando a otra pregunta, en general, los *rankings* son muy engañosos y depende de los parámetros en los que nos fijemos, obtendremos resultados diferentes. Por eso, los *rankings* o las estadísticas también son engañosos. Lo que sí sabemos es que el número de incidentes de ciberseguridad es muy preocupante y, como dije al principio de mi intervención, creemos que la principal amenaza para la seguridad nacional son las ciberamenazas, junto con el terrorismo yihadista. Les agradezco que muchos me hayan tachado de optimista —que lo soy—, pero, como dije en mi primera intervención, no hay mayor problema para la seguridad nacional, junto con el terrorismo, que las ciberamenazas. Es decir, somos plenamente conscientes de que nos enfrentamos a un grandísimo problema, sobre el que hemos empezado a actuar hace nada, tanto nosotros como los franceses, los portugueses y los ingleses. Es decir, en el mundo se ha empezado a actuar contra las ciberamenazas desde hace muy poquito tiempo. Cuando hablamos de estadísticas y nos referimos al puesto 19, 18 o 17, no estamos hablando de la liga, no es la *champions,* pero sí que podemos decir que nos encontramos en el vagón de cabeza de los países avanzados, pero nos ocurre lo mismo en muchas materias. España es un país avanzado tecnológicamente; habrá países más avanzados, pero hay muchísimos más países menos avanzados. También los países más avanzados sufren más ciberataques, es normal. ¿Qué países sufren más ciberataques? Estados Unidos, Alemania, Reino Unido, España; es decir, los países que están conectados digitalmente. Por eso, todo lo relativo a estadísticas y a *rankings* en materia de ciberseguridad puede llevar a engaño, pero siempre es bueno tener referencias y ahí están.

Podemos decir que España, tecnológicamente, es un país avanzado y en ciberseguridad también lo es en comparación con el resto, pero en gran desventaja frente a las amenazas a las que nos enfrentamos; todos estamos en gran desventaja. Como decía al principio de mi intervención, son las dos caras de una moneda. En España, frente al terrorismo —que, desgraciadamente ha costado muchísimo sufrimiento—, se han desarrollado unas capacidades, una organización y una estructura muy grande, si bien, a pesar de todo, hemos visto que la seguridad absoluta no existe y han sucedido atentados como los recientes de Barcelona y Cambrils. Cuando analizamos la ciberseguridad, junto al terrorismo, vimos que no había nada.

En cuanto a la obligación de comunicar respecto de las directivas, tanto el Reglamento de Protección de Datos de la Unión Europea como la Directiva NIS van a establecer la obligatoriedad de comunicar e incluso se establecerán sanciones para las empresas que no lo comuniquen. Muchas veces no se quieren comunicar los incidentes, entre otras cosas, porque lleva acarreado, generalmente, un daño reputacional.

cve: DSCG-12-CM-54

Si, como es el caso de Deloitte, se hace público y se extiende que le han robado los datos de sus clientes, etcétera, el perjuicio para la empresa es grande. Es decir, cualquier empresa va a intentar no comunicar, pero los trabajos de trasposición de la Directiva NIS van a llevar acarreadas unas sanciones para aquellas empresas que no comuniquen que han sufrido un incidente de este tipo.

Respecto del personal cualificado, he de decir que es un gran problema. Se suele decir —lo dicen los grandes gurús del mundo— que vivimos una revolución tecnológica exponencial, que el mundo va a cambiar en diez años drásticamente y se van a generar nuevos empleos. Vivimos en un momento en el que el mundo está en continua evolución, pero quizás lo que es llamativo de este momento que nos ha tocado vivir es la velocidad de ese cambio, y esa velocidad va a llevar aparejada la destrucción de los puestos de trabajo tradicionales y la creación de nuevos; es decir, llevará aparejada una transformación profunda de nuestra sociedad, una transformación hacia lo digital. También antes se comentaba si todos los jueces deberían tener una gran formación en este tipo de delitos, porque al final todo acabará así. Probablemente sí, exagerando. Cualquier profesión tendrá que tener conocimientos. Si somos médicos, también tendremos que tener un profundo conocimiento tecnológico; si somos abogados, si somos juristas —ustedes se han referido en infinidad de ocasiones a la regulación, a la legislación—, tendremos que tener una especialización en este mundo, etcétera. Es decir, todo, en general, avanza hacia esa digitalización de la sociedad, hacia esa revolución tecnológica que también supondrá unas transformaciones muy grandes en el mundo de la seguridad, unas transformaciones en lo que entendemos por ciberseguridad.

Respecto a las comunidades autónomas, en esto estamos creciendo todos juntos. Uno de los mayores esfuerzos es crecer coordinadamente dentro de nuestro país y también en las organizaciones de las que somos parte. ¿Qué es lo que pasa? Que entre edificios construidos —por así decirlo— es más fácil coordinarse. Cuando todos estamos haciendo estructuras, organismos, organizaciones y cosas nuevas es más difícil. Casi nada de lo que yo hablo aquí tiene más de diez años. En concreto, dentro de nuestro país es el Centro Criptológico Nacional el que tiene encomendada la seguridad de la Administración y mantiene contactos con los centros equivalentes de las comunidades autónomas. Sé que existe una buena comunicación, por supuesto mejorable, a nivel técnico. En general, en este mundo existe mayor coordinación a nivel técnico porque es más fácil; existe mayor coordinación a nivel técnico que a niveles superiores. De todas formas, la Ley de Seguridad Nacional también establece un mecanismo de coordinación con las comunidades autónomas; establece una Comisión para la seguridad nacional con las comunidades autónomas.

En referencia a las preguntas del señor Legarda, del Grupo Vasco, como él decía, estamos tratando una amenaza vital para nuestra seguridad; no puede ser más cierta su afirmación. También se refería a las comunidades autónomas y yo creo que al menos he indicado un poco en lo que estamos trabajando. Sobre Europa voy a poner un ejemplo práctico, el del caso del WannaCry. Cuando sucedió el ataque WannaCry, al que la señora Vázquez se ha referido, creo que en España se actuó francamente bien. De hecho, me gustaría poner encima de la mesa que, a las pocas horas de conocerse el ataque, España, en concreto el Centro Criptológico Nacional, puso una vacuna a disposición de todas las empresas nacionales y de todas las empresas del mundo para que no se extendiese ese ataque. Fue el primer organismo en el mundo que suministró a la sociedad una vacuna, lo que habla muy bien de la capacitación de nuestros profesionales. Fue un ataque que tuvo más repercusión mediática de lo que en sí supuso para las empresas porque no afectó a los servicios esenciales. Afectó a alguna empresa y enseguida apareció en los telediarios, pero no tuvo mucha repercusión más allá de que se apagaran los ordenadores. Fue más una repercusión mediática. En las primeras horas pulsamos las empresas y vimos que las cosas se estaban haciendo bien, dentro de que siempre en cualquier crisis de este tipo en las primeras horas hay un poco de descontrol. Las cosas se hicieron bien y dijimos: vamos a contactar con Europa. Teníamos una buena relación con otros países, pero a nivel Unión Europea ese edificio tampoco está hecho, y a un nivel político-estratégico de alto nivel como el nuestro encontrar en Europa un interlocutor que nos hable por la Unión Europea ahora mismo no es posible porque no existe. Existe a nivel técnico. Los centros técnicos sí tienen homólogos en los países con los que existe una buena comunicación y con los que nos apoyamos, etcétera. Pero en concreto en la ciberseguridad, no. El Departamento de Seguridad Nacional es el punto de contacto de España para la gestión de crisis. Ya me he referido en concreto al caso de la ciberseguridad, pero el punto de contacto en España para la gestión de crisis es el Departamento de Seguridad Nacional, la Secretaría Técnica del Consejo de Seguridad Nacional. Pues igual que cuando

cve: DSCG-12-CM-54

pasan crisis en Europa en otros ámbitos tenemos una estructura, que funcionará mejor o peor, pero tenemos un camino, en el caso de la ciberseguridad todavía no existe.

Me preguntaba sobre el voto electrónico. Refiriéndome también al WannaCry, Reino Unido, que en un esfuerzo de *marketing* alardea —y probablemente sea verdad— de que es uno de los países que más gasta en ciberseguridad, fue uno de los países más afectados, donde el WannaCry afectó a muchísimos hospitales. En una reunión que tuvimos, alguien se planteaba el caso curioso —un poco en plan de broma— de cómo en muchos hospitales se ha ido digitalizando todo, informatizando todo, y, entonces, al pasar un caso como el de WannaCry, se dijo que habría que volver a la tablilla que había en la cama del enfermo, porque en un caso como este no sabemos ya ni lo que tiene el enfermo al haberse perdido todos los datos. Respecto al voto electrónico —siendo prudente, porque en estas cosas el sentido común siempre recomienda la prudencia ante cosas tan importantes—, probablemente será una adaptación progresiva en el que haya sistemas tradicionales junto a sistemas electrónicos que permitan la comparación. Es una opinión sensata, no veo que sea ahora el momento de lanzarse a un voto masivo y jugar todo a esa carta, sino una evolución tranquila hacia un sistema electrónico.

En relación con las cuestiones que ha planteado el señor Gutiérrez, del Grupo Ciudadanos, hay un tema fundamental, que es la concienciación en el tema de la cultura; es fundamental, quizás el tema más importante de cara al futuro. Son temas sobre los que no se obtienen resultados de un mes para otro o de un año para otro, son temas a largo plazo. En el Departamento de Seguridad Nacional realmente estamos haciendo un gran esfuerzo en este tema, porque lo consideramos fundamental. Siempre que he hablado de ello he puesto el mismo ejemplo, que es el de la seguridad vial en España. Permítanme que ponga mi ejemplo: cuando yo iba en coche con mi padre, mi actitud en la carretera era decirle a mi padre que tenía que adelantar, pero ahora voy en coche con mis hijos y, como tenga el menor despiste, mis hijos me llaman la atención. Ha habido un cambio tremendo de mentalidad en una generación y eso ha sido gracias a campañas y a invertir dinero, no se ha producido por generación espontánea; ha habido un gran esfuerzo que creo que ha dado grandes resultados, o por lo menos yo lo aprecio en mi ejemplo: la mentalidad en este campo desde que yo era un niño a ahora —lo veo en mis hijos— ha cambiado infinitamente. Creo que en el campo de la seguridad en general y en el caso concreto de la ciberseguridad hay que emprender una campaña de este tipo, porque el mal uso o el uso irresponsable de la tecnología, que lo va a inundar todo, puede causar grandes perjuicios. Somos conscientes de ello y en la próxima Estrategia de Seguridad Nacional, en la que se está trabajando ahora, uno de sus puntos y objetivos fundamentales será la cultura de seguridad nacional, una cultura que abrirá un paraguas para muchos otros temas, como cultura de defensa nacional, cultura de ciberseguridad, etcétera. Los resultados son mejorables, estamos empezando, pero por lo menos existe esa conciencia clara de que es un tema crucial.

Hemos hablado de lo que invierten muchos organismos. Ahora, en general, casi todas las campañas las está haciendo el Incibe, el Instituto Nacional de Ciberseguridad, que, dentro de la Administración, es el organismo encargado de la ciberseguridad para ciudadanos y empresas. El Incibe tiene un presupuesto dedicado precisamente a las campañas de concienciación. Posiblemente, sea un presupuesto escaso y, previsiblemente, a medida que somos conscientes a todos los niveles —de ahí la importancia de que ustedes sean conscientes porque si yo lo soy y ustedes no, no voy a conseguir nada, porque precisamente las regulaciones están de su parte y no de la mía—, se irá invirtiendo más dinero y podremos conseguir ese cambio de mentalidad que en otros ámbitos había.

Se refería a la ISO 27001. Haré una pequeña aclaración. Dentro de la Administración, es obligatorio el cumplimiento del Esquema Nacional de Ciberseguridad, que viene a ser lo que la ISO a la Administración. En ese caso, respecto al grado de implantación, tengo unos datos —me han calificado muchas veces de optimista— que no son tan dramáticos como los suyos. Alrededor de 355 organismos públicos han implantado el Esquema Nacional de Seguridad y la cifra en las comunidades autónomas es alrededor del 66 %. Es decir, se está implantando, es una labor que hace el Centro Criptológico Nacional, responsable de la ciberseguridad para las administraciones públicas. Volviendo a la concienciación, dentro de las administraciones o de las empresas la concienciación de los altos niveles es fundamental. Que el Esquema Nacional de Seguridad se aplique en la Administración o que la ISO se aplique en una empresa depende del grado de concienciación que tenga el ministro o el CEO de la empresa; depende de que un ministro diga que ese tema es importante y que quiere tenerlo mañana implantado o que el CEO de una empresa diga que la ISO 27001 esté implantada. ¿Eso qué es? Concienciación. Hemos tenido muchas reuniones con responsables de ciberseguridad de empresas y al hablar de la Directiva NIS —porque tenemos consultas con el sector privado— les digo que para su sector es una oportunidad enorme porque

cve: DSCG-12-CM-54

va a hacer que en su empresa no les vean como los raros, los friquis, unos tipos rarísimos que saben de cosas rarísimas. Así, al final, si no son capaces de evaluar las pérdidas económicas que supone para una empresa —Deloitte seguro que sí es capaz ahora de evaluar las pérdidas si eso se ha publicado—, por lo menos va a haber una legislación que obligue a esa empresa a una serie de cosas, como en el caso del Reglamento de Protección de Datos obliga a las empresas a tener la figura de un jefe de protección de datos de la empresa, es decir, alguien que vela por que se cumplan los reglamentos, por que se hagan evaluaciones, etcétera.

Otro campo importante que va a empujar todo esto van a ser los seguros, porque a la hora de asegurar, las compañías de seguros van a exigir unos requisitos: usted tiene que cumplir esto y esto. Si le aseguro la casa y tiene una alarma y unas rejas, su seguro va a ser mejor que si no las tiene. Todo lleva, poco a poco, a una mayor regulación y a un mayor entendimiento, pero son procesos lentos por lo que a veces no obtenemos los resultados de forma rápida.

Respecto a la pregunta sobre los juzgados, le diré que hay una unidad en la fiscalía especializada en delitos cibernéticos. En los últimos años se ha avanzado muchísimo; avances que vienen con nombres y apellidos. Ha avanzado muchísimo y ha habido modificaciones del Código Penal, etcétera. En este campo queda mucho por hacer porque es muy difícil, es un tema extremadamente complicado pero se está en el camino, en el *safe harbor*. Como se suele decir, vivimos en casas de cristal. No sé dónde leí hace años que la mayor base de datos del mundo la tenía una cadena de supermercados en Estados Unidos, porque a través de la tarjeta de puntos tenía datos de no sé cuántos millones de norteamericanos. Nuestros datos están en todas partes, algo desproporcionado, y, además, a lo mejor no los tiene una agencia de seguridad, sino que los tiene una multinacional de supermercados. Se está avanzando, hay un Reglamento de Protección de Datos y está la concienciación.

Ahora contestaré a lo que ha planteado el señor Comorera, de Unidos Podemos, sobre la posibilidad de involucrar a la sociedad en esa protección de datos. Yo creo que casi todos los procesos que se inician hoy en día son más inclusivos, es decir, tienden a considerar más a las empresas. En el propio Departamento de Seguridad Nacional nosotros hemos coordinado las últimas estrategias que ha habido en España: la Estrategia de Seguridad Nacional de Ciberseguridad, la Estrategia de Seguridad Marítima Nacional, etcétera, y cada vez somos más conscientes de la necesaria implicación del sector privado. En los trabajos de la Estrategia de Seguridad Nacional la participación del sector privado ha crecido muchísimo respecto a todas las estrategias anteriores de seguridad nacional. ¿Por qué? Porque es necesario completar muchísimos aspectos.

En cuanto a la formación, efectivamente es necesaria —creo que ya lo he contestado antes—, pero la formación lo es en todos los ámbitos, también para un médico o para las Fuerzas y Cuerpos de Seguridad del Estado, que tienen que seguir haciendo un esfuerzo. Muchas veces varía el peso, es decir, a lo mejor durante unas épocas existe un determinado tipo de delitos, etcétera, que demandan una mayor especialización en determinados temas y muchos de esos efectivos que se dedicaban a eso se trasvasan a otras actividades. Lo que está claro es que hoy en día a casi todos los delitos —como decía en mi intervención— hay que ponerles ciber, casi todo es ciber. La razón es facilísima, es lo que ofrece una rentabilidad mayor a un menor riesgo.

Ya me he referido a la formación y los juzgados. En cuanto a la injerencia del Estado en las campañas de influencia —a lo que varios grupos han hecho referencia—, yo tengo que ser cauto, tengo que ser prudente en las afirmaciones, pero muchos indicios llevan a que determinadas acciones van orientadas claramente a la consecución de unos fines determinados, está claro que existe. Hemos dicho que esto ha existido toda la vida por unos medios o por otros. ¿Hoy en día por dónde se realiza la actividad humana fundamentalmente? Por el ciberespacio. ¿Por dónde se va a tratar de ejercer esta influencia? Por el ciberespacio.

Hay algunas opiniones influyentes, como la del señor Assange, por ejemplo. Yo me limitaré a dar datos contrastados. Por ejemplo, la auditoría de Twitter dice que la mitad de sus seguidores son robots; tiene una fuerza propagandística tremenda, porque hay ahí es una maquinaria propagandística. En cuanto a sus relaciones, sus conexiones, yo no tengo datos contrastados para poner encima de la mesa, pero sí sorprende por determinados alineamientos, determinadas circunstancias. Si toda la vida ha habido espionaje industrial, ahora es ciberespionaje; si toda la vida ha habido espionaje entre Estados, ahora es ciberespionaje. Es decir, la actividad humana se va desplazando a este campo y viene haciendo lo que se venía haciendo continuamente, solo que ahora se viene realizando por esas facilidades que da el ciberespacio, lo que pasa es que si yo quiero influir sobre un gran número de personas, encima tengo la

cve: DSCG-12-CM-54

posibilidad de hacerlo, con muy poquito dinero; con muy poquitos medios puedo influir; si tengo la voluntad de hacerlo, lo puedo hacer fácilmente.

Respecto a lo que ha planteado el señor Hernando, del Grupo Parlamentario Socialista, sobre los medios, estos siempre son escasos por definición; eso es para cualquiera que nos pregunte. Cuando se crea la Estrategia de Ciberseguridad Nacional, en diciembre de 2013, con crisis económica, lo que realmente se intenta es una reasignación dentro de cada organismo, es decir, se crea por ejemplo un mando conjunto de ciberdefensa dentro del Ministerio de Defensa con los presupuestos que ya tenía el Ministerio de Defensa, pero se ha creído conveniente que ante el panorama estratégico, etcétera, las Fuerzas Armadas debían tener un mando conjunto de ciberdefensa, en un momento en el que el presupuesto de las Fuerzas Armadas iba disminuyendo, pero se priorizó contar con esa capacidad operativa, y lo mismo en las Fuerzas y Cuerpos de Seguridad del Estado, etcétera. ¿Qué ha pasado? A medida que se ha ido superando la crisis económica el dinero ha sido mayor y se han fortalecido capacidades, en concreto, el Centro Criptológico Nacional y el Centro Nacional de Inteligencia, en dinero y en personas, y ahí aparece la dificultad de encontrar personal cualificado.

Si nosotros ahora quisiésemos contratar en la Administración a muchísimo personal con cualificación en este ámbito, nos sería imposible en España porque no existe. Es uno de los grandes problemas y por eso lo he puesto de manifiesto. Sí existe un plan detallado de lo que hace falta en España a raíz de los trabajos del Consejo Nacional de Ciberseguridad, donde se hizo un estudio de qué medios y recursos, tanto materiales como humanos, harían falta. Es una primera pieza para saber dónde debemos gastar el dinero. Para hacer una inversión necesitamos saber primero dónde la hacemos; no podemos asignarla a lo loco, sino asignarla con cabeza, ver lo que hace falta y buscar sinergias. Esto se ha pensado dentro del Consejo Nacional de Ciberseguridad, donde hay un estudio que así lo contempla y que es el referente a la hora de asignar recursos.

Respecto a las culturas departamentales, hay que decir que es algo inherente. Nosotros somos afortunados, porque si tuviéramos tantas agencias como los Estados Unidos nos volveríamos locos. Nosotros, afortunadamente, somos pocos, pero es normal que en todos los países del mundo exista competencia sana entre agencias, que en muchos casos es un acicate y en otros casos puede ser perjudicial. ¿Qué es lo que pasa en la ciberseguridad? Que es algo muy transversal. Podrían estar involucrados el Ministerio de Defensa, el Ministerio del Interior, el Ministerio de Industria, prácticamente todos los sectores, el de economía, la justicia... ¿Qué es lo que se produce en España desde el año 2013? España cuenta con la Estrategia de Seguridad Nacional que crea el Consejo de Seguridad Nacional, que precisamente lo que hace poner en una mesa a todos los actores al más alto nivel, porque la implicación si no es al más alto nivel es muy difícil, y quedan los órganos de apoyo, como es el Consejo Nacional de Ciberseguridad que es donde se sientan en la misma mesa todas esas culturas departamentales para fijar unos objetivos comunes. Venimos trabajando desde el año 2014 en solventar eso, en coordinarnos, en problemas de agencias, etcétera. Pasa en todos los países del mundo, y en Estados Unidos es asombroso por la cantidad de agencias que hay. Los nuestros, al fin y al cabo, son manejables, pero precisamente las estructuras que se están poniendo en práctica en España son para solventar esos problemas, para crear sinergias. ¿Dónde hemos actuado nosotros, el Departamento de Seguridad Nacional? En defensa nacional España tiene unas estructuras muy consolidadas, quizá por la lucha contra el terrorismo, desgraciadamente, después de muchísimos años de lucha contra el terrorismo. ¿Dónde no existía esa gobernanza? Pues en el caso de la ciberseguridad y en otros casos, se han creado esas estructuras, esa gobernanza nueva ante problemas nuevos, porque no existían: Consejo de Seguridad Nacional, Consejo de Ciberseguridad, Comité Anticrisis, donde todos juntos nos sentamos. Por tanto, creo que es verdad que esas culturas departamentales son parte de un problema, que es lógico, pero es algo que ahora mismo yo creo que en España tenemos solucionado. Siempre van a existir, porque es así, y a veces también es bueno.

Sobre los agentes estatales, es un poco lo que he dicho. Si un país siempre ha querido ejercer influencia sobre otro pues ahora tiene todos los medios para hacerlo. Es la voluntad. ¿Que en España o en Europa ha habido campañas? Pues la lógica dice que sí. Me he referido muchísimas veces a la dificultad de atribuir las acciones. Por eso hay que ser prudentes a la hora de atribuir acciones. Cuando ciertas acciones van orientadas a un determinado fin y de una forma determinada, se puede sospechar que se está produciendo. ¿Qué es lo que pasa? Que ante muchas cosas, con todo lo de la ciberseguridad, es muy difícil luego que un Gobierno acuse delante de un juez a otro Gobierno y decir: Usted ha hecho esto. Eso es algo muy difícil. Pero es un fenómeno que se está produciendo, y dentro de la Unión Europea

cve: DSCG-12-CM-54

y dentro de la OTAN se está evaluando esto como una de las cuestiones más preocupantes. Es lo que se conoce como los conflictos híbridos, donde junto a las capacidades militares se desarrollan estas operaciones de influencia como una parte normal de una operación militar o de un intento de desestabilización, etcétera. Es algo que está ahí, que es verdad, aunque no me voy a referir a ningún caso en concreto, porque habría que poner un dato encima de la mesa que yo no tengo.

La señora Vázquez, del Grupo Popular, me ha planteado varias cuestiones como la captación del talento. Sí se están tomando iniciativas. Antes me referí al Instituto Nacional de Ciberseguridad que, en concreto, tiene una actividad que es el CyberCamp, que realiza todos los años y que está especialmente dedicada a la captación de talento entre jóvenes, etcétera. Probablemente sea necesario todavía más porque el problema es muy grande, quiero decir la falta de profesionales en este campo. En cuanto a si son suficientes los recursos que se destinan a ello, probablemente sea necesario destinar más. En general, tanto la captación del talento como la formación de profesionales en ciberseguridad es algo que yo creo que, como todo, es un mundo que está apareciendo nuevo, que está evolucionando muy rápido, y la luz roja de la falta de profesionales en la ciberseguridad se enciende hace muy poco. Hace cinco años, por ejemplo, nadie hablaba de que en España no había suficiente número de profesionales de la ciberseguridad, nadie. Intenten buscar cualquier periódico de hace cinco años que ponga este problema encima de la mesa, y verán que es algo que ha aparecido hace un año o año y medio. Es que todo es muy nuevo y va muy rápido.

Había hecho referencia, además, a un tema sobre la creación de una reserva estratégica, que yo creo que es una idea buena. Falta ver cómo se materializa. Puede ser buena o mala según su materialización, pero tampoco una reserva puede ser el pilar de la ciberseguridad en España. Por ejemplo, la reserva que existe en las Fuerzas Armadas es un complemento de las actividades de las Fuerzas Armadas y, en algunos casos, muy útil, por ejemplo, en el caso de los médicos. Las Fuerzas Armadas, que tienen numerosas misiones en el exterior y tienen muchísimos barcos navegando largas navegaciones fuera de España, demandan un número de personal sanitario muy grande; un personal sanitario que tampoco las Fuerzas Armadas necesitan que estén treinta años, sino para que cumplan unos servicios determinados. En este caso del personal sanitario de las Fuerzas Armadas, la reserva que queda establecida es de gran ayuda. Similarmente podría ser en el caso de la ciberseguridad, podría complementar determinados aspectos de la ciberseguridad. Ahora bien, yo no lo veo como para que sea un pilar básico de la ciberseguridad en España, sino que sea algo que complemente a lo que ya hay y que será muy útil. A la gente le gusta participar también, y mucha gente que sirve en la reserva de las Fuerzas Armadas está muy gustosa de participar, de poder servir o poder ayudar, en definitiva.

La colaboración público-privada es un asunto dificilísimo; para empezar, porque lo privado es amplísimo. Es que dentro de lo privado está la universidad, las empresas, etcétera. Entonces, claro, la colaboración público-privada es algo que está ahí y que todos queremos mejorar, pero luego es muy difícil. Nosotros, en la ciberseguridad, desde un principio, hemos contado mucho con el sector privado; pero no con todo el sector privado. Por ejemplo, en España hay infinidad de pymes, no sé el dato, pero involucrar a todas las pymes en esto de la ciberseguridad es muy difícil porque hay un volumen tremendo en las grandes empresas o las empresas que sustentan servicios esenciales.

Perdón, me ha olvidado de una pregunta del señor Hernando sobre la Oficina de Coordinación Cibernética. La Oficina de Coordinación Cibernética ejerce la coordinación dentro de lo que recoge la Ley de Infraestructuras Criticas y el Ministerio del Interior, pero fuera de eso no coordina nada más que lo que está dentro de su ámbito. El Consejo de Seguridad Nacional, que preside el presidente el Gobierno, coordina todas las iniciativas que están en el ámbito de la Administración. Es decir, es algo muy, muy superior a la Oficina de Coordinación Cibernética, que tiene un determinado rango, pero no con la capacidad de coordinar toda la ciberseguridad de un país; no está pensada para eso ni tiene capacidad.

Se habla del Consejo de Seguridad Nacional, en primer lugar, porque en él está la figura del presidente del Gobierno, y luego hay una secretaría técnica, que es el Departamento de Seguridad Nacional, que en la práctica ejerce esas funciones, pero la actuación de la Oficina de Coordinación Cibernética está pensada dentro de las infraestructuras críticas y dentro del Ministerio del Interior fundamentalmente para coordinar las unidades de Policía, Guardia Civil y del CERT de Seguridad e Industria, pero más allá de eso, no tiene ni capacidad ni intención de hacerlo.

La señora Vázquez se ha referido además a la coordinación de las unidades dentro del Ministerio de Defensa. Yo, que soy oficial de la Armada, les digo que hay distintas culturas departamentales, y en este sentido el ámbito de las Fuerzas Armadas es muy grande. En 2014 se crea un organismo nuevo,

cve: DSCG-12-CM-54

dependiente del jefe del Estado Mayor de la Defensa, y tiene que coordinar las capacidades de tres ejércitos y coordinarse con los actores exteriores, por lo que el campo para actuar y mejorar es enorme, ya que a pesar de que se crea en el año 2014, realmente operativo, funcionando con todas sus capacidades a pleno rendimiento, debe llevar año y medio. Por tanto, cada vez asumirá más roles, cada vez asumirá más funciones y cada vez tendrá una mayor capacidad de coordinar o de concentrar las capacidades de las Fuerzas Armadas en un único organismo.

De todas formas, en las Fuerzas Armadas las peculiaridades son muy grandes, porque la coordinación para la Armada, por ejemplo, de unidades navales es muy distinta que la ciberseguridad que puede necesitar el Ejército del Aire en sus peculiaridades, etcétera. No obstante, existe un ámbito común grande, que es lo que el Mando Conjunto de Ciberseguridad y Defensa trata de desarrollar. Perdón que siempre insista sobre el mismo tema, pero esto es algo que va creciendo, va evolucionando, se va construyendo, porque lleva operativo poco más de un año.

Creo que, más o menos, me he referido a las demás cuestiones, pero sí quiero hablar sobre cómo afectaría a España la Agencia Europea de Ciberseguridad. Hay un fenómeno que creo que es bastante acertado y que es crear organismos específicos de ciberseguridad. La ciberseguridad ha venido para quedarse, es decir, el riesgo de ciberamenazas va a ser cada vez mayor y va a dedicar una mayor especialización, va a requerir cada vez más recursos, va a requerir cada vez más personal, y es lógico que se vayan constituyendo unidades u organismos dedicados en exclusiva a la ciberseguridad como tal. Que exista una Agencia Europea de Ciberseguridad ayudará mucho, porque, por ejemplo, en el caso del Wanna Cry, al que me refería, nosotros, que estábamos pendientes de cómo se estaba tratando el problema en España, podemos decir que tuvo casi más repercusión mediática que real. Que una empresa grande ordene a sus empleados que apaguen el ordenador y salgan, y esto aparezca en el telediario de las tres de la tarde, tiene repercusión, pero técnicamente a las pocas horas se encontró una vacuna y ningún servicio esencial en España resultó afectado. Si se quisiese comprobar qué está pasando por ahí y si esta Agencia de Ciberseguridad existiera, tendríamos un interlocutor que a nivel de la Unión Europea podría evaluar qué está pasando y buscar —porque para eso se crea a nivel europeo— sinergias, etcétera, etcétera.

No sé si me dejo alguna cuestión en el tintero. En cualquier caso, les agradezco mucho sus comentarios, que creo que son muy acertados, y en el Departamento de Seguridad Nacional de la Presidencia del Gobierno estamos a su completa disposición para todo lo que quieran.

Muchísimas gracias.

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

Por si se ha quedado alguna pregunta en el tintero, voy a abrir un segundo turno en el que los portavoces puedan aclarar, matizar o ampliar las preguntas que han hecho. ¿El señor Yanguas quiere utilizar el segundo turno? **(Denegación).** ¿El señor Legarda quiere utilizar el segundo turno? **(Pausa).** No está. ¿Señor Gutiérrez?

El señor **GUTIÉRREZ VIVAS:** Sí, gracias, presidente.

En primer lugar, es un placer charlar y debatir con el señor Castellón; se nota que sabe de lo que está hablando y esto es algo que siempre se agradece profundamente.

Solamente quiero matizar dos cosas. En primer lugar, aquí comparecerán los señores de Incibe. Creo que están haciendo una labor magnífica, tiene usted toda la razón. La verdad es que el CyberCamp de Incibe es magnífico y es un espacio de detección de talento precoz que creo que es la línea. La amenaza, como ya hemos comentado, va a ser cada vez más grande y, de hecho, el Internet de las cosas lo único que va a hacer es favorecer esta amenaza de una forma tremenda. Al final, cuantos más dispositivos conectados tengamos más probabilidades de que la amenaza sea más grande y esto va a tener mucho que ver con eso. Aquí es donde la Administración tiene que trabajar también para que nuestro tejido empresarial sea capaz de dar solución a esta amenaza, no solo desde la autoprotección del tejido empresarial, sino también el fomentar, como decíamos antes, que se cree una empresa tecnológica. Aquí hay un ejemplo y un modelo que es Israel, que siendo un pequeño país ha conseguido ponerse de forma puntera en cuanto a la especialización, por ejemplo, en ciberseguridad, no solo en *software* sino incluso en *hardware*. Me gustaría apuntar a que esto va por aquí.

Sobre lo que me decía usted del esquema de seguridad nacional para las empresas, sobre todo la Administración, lo conocemos; sabemos que existe y que la Administración está usándolo, pero para mí tiene un déficit respecto de una norma ISO y es que no es auditable. Al final es una cosa que se acoge

cve: DSCG-12-CM-54

con una serie de normas que están decididas en el esquema nacional de seguridad y entonces la Administración las cumple o no, pero esto no es auditable. Como usted bien conoce, si la norma, si los sistemas no se actualizan, si los parches no se instalan en los sistemas operativos, en los programas, esa norma acaba quedando desactualizada. Precisamente lo que garantiza una norma ISO o cualquier otra entidad —no quiero yo hacer publicidad aquí de la norma ISO— es que al ser certificable con periodicidad anual o bianual al final lo que hace es que la empresa, en este caso la Administración, se deba de preocupar de invertir en que sus sistemas estén a punto. Por eso hago esta diferencia que me parece correcta.

Finalmente, dos cosas. La Administración tiene el CIO desde hace no muchos años. Creo que ha sido un gran acierto que la Administración tenga el CIO, tenga un director de sistemas de información —por fin— para toda la Administración. Creo que le falta un CSO, un Ship Security Officer*;* creo que la Administración debería tener también y debería identificar esta figura porque será la manera en que la Administración acabará instalando sistemas de protección.

Acabo. Me gusta la comparación del CEO y el ministro lo que pasa es que, lamentablemente, cuando el CEO no lo hace bien y los sistemas son hackeados el consejo de administración o el consejero delegado hace dimitir al CIO; quizá el presidente del Gobierno tendría que haber hecho dimitir al ministro de Justicia. Por eso creo que esas comparaciones son siempre peligrosas.

Muchísimas gracias.

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

Señor Comorera, ¿quiere intervenir?

El señor **COMORERA ESTARELLAS:** Sí, con brevedad, presidente.

La única pregunta que creo que no me ha contestado es sobre si considera necesaria alguna reforma legislativa ahora mismo; es lo que me ha parecido que no me ha contestado en toda su exposición.

Por otra parte, nos ha hecho una distinción entre hackers y crackers. Lo digo porque en muchos países aquellos hackers que de alguna manera descubren determinados agujeros de seguridad, o lo que sea, desde la Administración se intenta colaborar con ellos. Recientemente, el pasado julio, tuvimos aquí el problema en relación con Lexnet y todo esto y la respuesta del Ministerio de Justicia fue comunicar que iba a denunciar a la persona que descubrió esta brecha de seguridad. Me gustaría que me diera su opinión al respecto.

Muchas gracias.

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

¿Señor Hernando? **(Denegación)**. ¿Señora Vázquez? **(Denegación)**.

Señor Castellón.

El señor **DIRECTOR OPERATIVO DEL DEPARTAMENTO DE SEGURIDAD NACIONAL** (Castellón Moreno): Muy brevemente.

Como bien ha referido el señor Gutiérrez, esta es la primera ponencia y por aquí pasarán, prácticamente, todos los expertos en ciberseguridad que hay en España. Creo que van a tener una ponencia de muchísimo nivel y podrán profundizar mucho más en cuestiones de la ciberseguridad en España sobre las que yo he pretendido dejarles una visión panorámica al respecto. Seguridad Nacional en España. Incibe —el señor Hernández vendrá aquí— es el encargado de impulsar esa industria. Está teniendo muchísimas iniciativas, está contando con un presupuesto para ello y yo creo que está bien orientado y que se están haciendo muchas cosas. Él podrá explicarle cuáles son sus objetivos, pero es algo que no ha pasado desapercibido; se está trabajando, aunque probablemente siempre es mejorable.

Sobre el Sistema Nacional de Seguridad, lo ideal sería establecer unos sistemas, unas auditorías más continuas. Ahora hay un gran esfuerzo en implementarlo, porque no está implementado al cien por cien. La acción del CIO, el señor Molina, junto con el Centro Criptológico Nacional, están haciendo un esfuerzo enorme en implementar el Esquema Nacional de Ciberseguridad. Cuando ese esquema tenga un nivel de implantación suficiente vendrá ir mejorando la auditoría, medir, etcétera, que es, por así decirlo, un paso lógico. Se está trabajando más en la implantación. Sobre esa figura del CIO, del director general, yo creo que en algún momento existirá una autoridad nacional de ciberseguridad. Igual que hablamos de la Agencia de Ciberseguridad de la Unión Europea, yo creo que en España en algún momento dado existirá una autoridad, se llame como se llame, que sea la autoridad de ciberseguridad en España, y que

cve: DSCG-12-CM-54

probablemente tendrá una orientación especializada en ciberseguridad. Muchas veces las ideas necesitan el tiempo propicio para llevarse a cabo, pero no tengo duda de que en algún momento existirá en España y prácticamente en todos los países de nuestro entorno.

En cuanto al Lexnet de justicia, cualquier incidente hoy en día está a dos minutos de una crisis por la conectividad, los medios de comunicación, etcétera. Cualquier cosa puede provocar una crisis. Yo creo que el incidente de Lexnet no es tan grande. ¿Qué es lo que ha producido, aparte de mucho ruido? ¿Se han filtrado expedientes, se ha filtrado algo realmente importante? Yo creo que no, a no ser que alguien me diga: es que apareció en WikiLeaks y en no sé qué. Yo creo que no ha aparecido nada importante en ningún lado, porque lo que comprendía Lexnet no eran expedientes, no eran sumarios, eran comunicaciones entre distintos organismos. Lo que produce es que es un fallo que dentro de la propia organización judicial unas personas que no tenían que tener acceso a determinada información de repente la tienen, pero es dentro del propio sistema judicial, y tienen acceso a una información que tampoco es demasiado relevante. Yo creo que el problema se ha querido magnificar porque es llamativo, para los medios de comunicación es un caramelo, pero ¿ha salido algo importante? Sincera y modestamente, yo no conozco ningún documento importante que se haya conocido por el caso Lexnet.

En España existe el Código Penal, y si una persona realiza una acción que está tipificada en el Código Penal lo lógico es que se le denuncie. Es más, para todas las personas, cuando presenciamos que alguien comete un delito, nuestra obligación es denunciarlo. El de Wanna Cry fue un hacker —las denominaciones dan igual— ético o como se quiera llamarlo, figura que a mí me gusta, me gusta ese mundo. Tú puedes actuar de una forma o de otra. Si tú lo publicas o actúas de forma que puede ser constitutiva de delito, al final te van a pillar porque estás proporcionando datos. Si estás dentro del Código Penal, ¿qué vas a hacer? En torno a Lexnet yo creo que se ha montado algo que es un ejemplo claro de la estrecha línea que separa un incidente de una crisis. Efectivamente, existían deficiencias en el sistema, que ahora mismo se están estudiando y poniendo todos los medios para que no se produzcan, pero los efectos que ha producido son muy pequeños. Es un efecto mediático. Yo no puedo decir nada. Si el Código Penal tipifica la acción de este señor, pues no sé.

En relación con la reforma legislativa, en este tema será continua. Precisamente, si hay algo que necesita ser reformado es esto. Nos pasa con la tecnología y con todo en general. En España, la Directiva NIS llevará aparejado un reglamento. ¿Qué vendrá a raíz de la Directiva NIS en Europa y en España? Nuevas estrategias de ciberseguridad, las cuales probablemente necesitarán otras, es decir, es un proceso continuo. ¿Se necesita una reforma legislativa? Sí, es una evolución. Probablemente, la Directiva NIS necesite ya una adaptación en muchísimos campos. Es una evolución continua y la falta de profesionales en este campo es constante. Ahora mismo no me viene a la cabeza como algo urgente, sino que es más un proceso: Directiva NIS, reglamento, ley, estrategias, una continua adaptación y en este campo mucho más.

El señor **PRESIDENTE:** Muchísimas gracias, señor Castellón.

No habiendo más temas en el orden del día, agradezco su asistencia y levantamos la sesión.

Eran las siete y quince minutos de la tarde.

cve: DSCG-12-CM-54