DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 102 | Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DEL EXCMO. SR. D. FERNANDO MARTÍNEZ-MAÍLLO TORIBIO, VICEPRESIDENTE SEGUNDO

Sesión núm. 17

celebrada el jueves 28 de junio de 2018 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

Comparecencias:

— **Del señor Maeztu Lacalle (abogado especializado en Internet, propiedad intelectual y tecnología), para informar sobre diversas cuestiones relativas a la ciberseguridad en España. Por acuerdo de la Comisión Mixta de Seguridad Nacional. (Número de expediente del Congreso de los Diputados 219/001288 y número de expediente del Senado 715/000533) 2**

— **Del señor León de Mora (director de la cátedra telefónica inteligencia en la red y director del Grupo de Investigación Tecnología Electrónica e Informática Industrial, TIC-150, de la Universidad de Sevilla), para informar sobre diversas cuestiones relativas a la ciberseguridad en España. Por acuerdo de la Comisión Mixta de Seguridad Nacional. (Número de expediente del Congreso de los Diputados 219/001289 y número de expediente del Senado 713/000992) 16**

— **De la señora Quintana (periodista experta en ciberseguridad, autora de los libros «Ciberactivismo», 2012, y «Ciberguerra», 2016, editorial Catarata), para que evalúe la situación actual de los derechos de los usuarios de Internet y las supuestas campañas de desinformación que constituyen supuestos ciberataques en contra de organismos públicos y privados en España. A petición del grupo parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea. (Número de expediente del Congreso de los Diputados 219/000932 y número de expediente del Senado 715/000321) 29**

---

cve: DSCG-12-CM-102

Se abre la sesión a la una y cinco minutos de la tarde.

COMPARECENCIAS:

— DEL SEÑOR MAEZTU LACALLE (ABOGADO ESPECIALIZADO EN INTERNET, PROPIEDAD INTELECTUAL Y TECNOLOGÍA), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/001288 y número de expediente del Senado 715/000533).

El señor **VICEPRESIDENTE** (Martínez-Maíllo Toribio): Buenas tardes a todos. Damos comienzo a la sesión de la Comisión Mixta de Seguridad Nacional. Como ven, no soy García-Margallo, es evidente, y estoy aquí por una razón lógica: él no podía venir, por tanto se ha excusado y he tenido que asumir yo la Presidencia en funciones. Espero que se desarrolle con la normalidad con la que siempre se ha desarrollado, bajo la Presidencia del señor García-Margallo.

Tenemos tres comparecientes, porque el cuarto, en este caso don José Carlos Moreno Durán, director de Inteligencia y Análisis del Grupo Santander, tiene un problema de disponibilidad y no podrá asistir. El procedimiento será el habitual, el compareciente intervendrá primero y luego iremos de menor a mayor. Según me han trasladado los portavoces de todos los grupos va a haber solo una intervención, que es lo que se ha acordado por parte de todos los grupos políticos, y yo voy a llevarlo a cabo.

Quiero dar la bienvenida al primer compareciente que me acompaña, don David Maeztu Lacalle, abogado especializado en Internet, propiedad intelectual y tecnología, para informar sobre diversas cuestiones relativas a la ciberseguridad en España. Le doy las gracias por su presencia en el Congreso de los Diputados en esta Comisión, y suya es la palabra.

El señor **MAEZTU LACALLE** (Abogado especializado en Internet, propiedad intelectual y tecnología)**:** Muchas gracias.

En primer lugar, lo que uno tiene que hacer es agradecer a sus señorías la presencia aquí, el interés por estos temas y por ampliar una cuestión como la seguridad nacional a aquellos que desde otra perspectiva o desde otro ámbito nos ocupamos también de determinados aspectos que a lo largo de mi intervención me permitiré mostrarles. Además lo primero que uno hace cuando se plantea venir aquí a exponerles algo es ver si puede transmitirles algunas experiencias o algunas consideraciones que uno a lo largo del ejercicio va haciendo. En atención a esto, y para que tengan en contexto el porqué de mis opiniones y de dónde nace lo que les voy a contar, he de decirles que soy abogado especializado desde el año 2004 en temas de derecho y tecnología, en temas de Internet, y he asistido a empresas en todo tipo de asuntos relacionados con la seguridad de la información: fugas de información, ataques de terceras empresas, problemas con sistemas de comunicación y seguros, he defendido y he asistido a *hacktivistas,* que es una de las cuestiones que a veces preocupan desde el punto de vista de la seguridad nacional, a empresas afectadas por ataques informáticos extremos, y últimamente, en el último año o año y medio me he centrado particularmente en el tema de las criptomonedas, *bitcoin* y todo lo relacionado, algo que sin duda les sonará y que puede tener importantes repercusiones en lo que desde el punto de vista de la financiación, el acceso a medios o a recursos por parte de grupos que puedan afectar a la seguridad nacional puedan hacer. Con todo este bagaje o con toda esta experiencia me presento, y someto a ustedes las consideraciones que, como digo, desde el desempeño habitual de mi trabajo, he podido reflexionar y trasladárselas de manera directa con la intención de que sean en provecho común.

La primera idea que quiero transmitir es la de la seguridad nacional como un concepto que comprende, tanto al mundo *on line* como al mundo *off line*. Es decir, vivimos en una sociedad hiperconectada en la que las cosas que suceden en Internet tienen un impacto en el mundo real, y las cosas que tienen impacto en el mundo real tienen un impacto en el mundo *on line;* como digo esto desde la ciberseguridad. Si nos preguntan si es un problema de ciberseguridad o si puede afectar a la seguridad nacional que una empresa que tiene una aplicación que se dedica a recoger la actividad que desarrollamos cuando hacemos deporte, que publica esos datos y hace mapas con esos datos, seguramente pensemos que no. Es decir, no hay un acceso ilegítimo a esos datos, no hay una vulneración de sus medidas de seguridad, sino que la empresa hace públicos unos mapas de calor con aquellos lugares por los que los usuarios corren, entrenan o realizan actividad física. Pues bien, en enero de este año esta empresa publicó unos mapas de calor que revelaron ubicaciones de bases militares, patrullas de militares patrullando determinadas zonas en Afganistán, en España y en otros muchos sitios, se podían establecer horarios de patrulla, rutas que en principio eran secretas o que no tenía por qué conocer nadie eran publicadas,

cve: DSCG-12-CM-102

etcétera. Es decir, no podemos considerar la ciberseguridad como una cosa que no va a afectar al mundo real y que no va a afectar a la seguridad, no son dos campos separados, no son dos campos diferenciados, no son dos campos que no tengan incidencia. Como decimos esta empresa de manera voluntaria ha publicado ubicaciones de bases militares, que en principio deberían estar protegidas, y se ha hecho accesible para cualquiera, que tratando esos datos ha podido acceder a la información que de alguna forma compromete la seguridad de todos. Por lo tanto esta situación, esta cuestión, estos aspectos que van a influir en todo aquello que les quiero exponer los vamos a ver de manera frecuente, de forma cada vez más habitual.

A lo largo de mi trabajo, en una ocasión —y vuelvo a la misma idea— asistí a una empresa que desarrollaba *software* para colegios profesionales. Cuando hablamos de seguridad, de proteger infraestructuras críticas, de desarrollar planes de contingencia frente a ataques o frente a intervenciones de terceros países o de cualquier interesado en dañar la seguridad, pensamos en proteger una central nuclear, en proteger una red de telecomunicaciones o una red de electricidad. ¿Qué tienen en común todos estos centros o todos estos lugares? Pues que para poder instalarlos pasan por un colegio profesional. ¿Protegemos la central nuclear y no protegemos el colegio profesional en el que se visa el proyecto para construir la central nuclear? ¿Protegemos el colegio profesional y no protegemos a los proveedores de *software* que van a gestionar la información almacenada en esos colegios profesionales? Es decir, no podemos tener una visión unitaria, única de la ciberseguridad como algo al margen de la seguridad. Por lo tanto entiendo que los trabajos de esta Comisión deben tener esa amplitud, esa visión, y por lo tanto debemos participar de todo ello.

Como todo esto permea, como todo esto afecta a cualquiera de nosotros, y como bien es sabido en temas de seguridad la cadena es tan débil como el eslabón más débil de la cadena, todos en algún momento dado podemos formar parte de ese eslabón, y todos en algún momento dado podemos debilitar la cadena. Estos dos ejemplos que he expuesto creo que lo evidencian. Pero hay cuestiones que deben trasladarse a aquellos que no están centrados en la seguridad o que no forman parte de ello, y hay mecanismos que sirven o deberían servir para simplificar esto.

En estas Cámaras se está tramitando ahora mismo un proyecto de ley orgánica de protección de datos. Seguro que conocen la reciente entrada en vigor o en aplicación del Reglamento General de Protección de Datos, esa armonización para toda Europa de la normativa que debe proteger los datos personales, que ha supuesto que quede en una especie de limbo jurídico la normativa que teníamos en España. ¿Qué tenía de bueno la anterior normativa que teníamos en España o la norma que había en España? Pues que las medidas de seguridad estaban pensadas y estaban definidas. Es decir, si yo, como persona, tengo que cumplir una serie de medidas de seguridad, por ejemplo el cifrado de la información, tener servidores en sitios seguros o almacenar la información de una determinada manera, en el momento en el que esas medidas quedan al arbitrio de las partes, al arbitrio de las personas, que a lo único que la norma obliga o exige es a que se adopten las medidas adecuadas y que no se pueda evaluar y que no esté claro, estamos debilitando una parte importante de la cadena, y por lo tanto estamos dando facilidades.

Yo les pediría que, en la medida de lo posible, en la tramitación de estas normas —que como he dicho está ahora mismo en esta Cámara—, primero, que se agilizase lo máximo posible, y segundo, que se recuperasen ciertas medidas de seguridad predefinidas, en la medida en que fuese compatible con el Reglamento General de Protección de Datos, para que las empresas, desde el punto más bajo hasta el punto más alto, tengan mecanismos claros de cómo proteger su información; porque como digo todo esto, al final, puede acabar afectando a bienes jurídicos superiores como en este caso la seguridad nacional.

Hay otra cuestión también relacionada con este aspecto de la seguridad jurídica como es, por ejemplo, la Ley de Conservación de Datos y la situación en la que estamos ahora. Para la prevención de ciertos delitos en Internet —como todos ustedes sabrán— es necesario poder identificar quién está detrás de una dirección IP o quién ha estado cerca de una antena de telecomunicaciones o a quién se le ha prestado un servicio de telecomunicaciones. Nuestra Ley 25/2007, que deriva de una directiva europea, fue anulada por el Tribunal de Justicia de la Unión Europea en el año 2014. Esta anulación de la directiva, sobre la base de ciertos principios que informan la Carta de Derechos Fundamentales de la Unión, ha provocado un limbo jurídico en varios puntos de Europa y está dificultando la investigación de delitos, de delitos graves y de todo tipo. En concreto en España esta norma no ha sido derogada, aunque hay resoluciones judiciales que manifiestan que no está vigente, y ha sido ampliada o reformada mediante la modificación de la Ley de Enjuiciamiento Criminal que se produjo en el año 2015. Sin embargo tenemos encima de la

cve: DSCG-12-CM-102

mesa una situación de inseguridad que se puede crear a partir de una cuestión prejudicial planteada por la Audiencia Provincial de Tarragona, en la que se cuestiona de alguna forma esta normativa. ¿Qué pasaría si el Tribunal de Justicia de la Unión Europea —en una resolución que está pendiente de recaer y que ya ha tenido el informe del abogado general— nos deja sin la posibilidad en determinados supuestos de acceder a esa norma o acceder a los datos que van a permitir resolver o proteger un interés vital de la Nación? Considero que es muy importante que se adopte una medida legislativa concreta que afecta a este aspecto, que como digo en principio puede no estar relacionada con la seguridad nacional, pero que puede llegar a tener una incidencia reseñable si en un momento dado los jueces o las Fuerzas y Cuerpos de Seguridad del Estado no pueden disponer de un mecanismo jurídico para poder resolver, investigar o proteger un determinado interés concreto. Por eso, antes de tener un problema por una anulación de esta norma, lo que deberíamos hacer es analizarla y adaptarla correctamente o asegurarnos de que está correctamente adaptada a lo que el Tribunal de Justicia de la Unión Europea dijo en el año 2014.

Por otra parte, la realidad en el mundo de Internet nos está llevando a que haya millones de dispositivos, decenas de lenguajes de programación, una evolución constante de las tecnologías. Si como digo todos formamos parte de la cadena y todos tenemos que procurar ser lo menos débiles posible, no podemos depender únicamente de la capacidad de los servicios militares o de los servicios de inteligencia para poder defendernos o para poder plantear las medidas adecuadas. Uno de los problemas que tenemos, que hemos detectado, en relación con lo que se denomina *hacktivismo* o los *hackers* o los *hackeos,* es que hay mucha gente que por simple curiosidad descubren fallos de seguridad. El término *hacking* hay que desmitificarlo un poco desde el punto de vista negativo, ya que el *hacking* puede venir directamente de la curiosidad, de la investigación, del conocimiento.

Quiero recordarles que el año pasado varias personas alertaron de un problema de seguridad con una aplicación que regula las comunicaciones por los juzgados, LexNET. Si una persona denuncia un fallo de seguridad en una aplicación, que en este caso afecta a algo tan importante como la justicia, corre el riesgo de ser procesada, que es lo que ha sucedido en este caso. No digo que se deba permitir que cualquiera entre en cualquier lugar. Lo que estamos haciendo los abogados es actuar de intermediarios. Cuando alguien descubre una brecha de seguridad o un problema de seguridad acude a nosotros y, amparados en el secreto de defensa o en el deber de secreto que tenemos respecto a nuestros clientes, somos nosotros los que notificamos las brechas de seguridad, precisamente para evitar que alguien que quiere colaborar, que no quiere hacer el mal, que solo quiere notificar un problema o un fallo de seguridad, porque fallos de seguridad los habrá, lo que tenemos que hacer es solucionarlos y no ampararnos en el desconocimiento pensando que está todo bien, cuando realmente el fallo existe. El fallo existe con independencia de que lo sepamos o no. Por eso digo que nosotros estamos colaborando precisamente notificando fallos de seguridad, para evitar y para permitir que estas personas sigan investigando, sigan desarrollando su tarea sin riesgo de ser enjuiciados o en su caso encarcelados. Esta es una cuestión que deberíamos también analizar y replantear. Necesitamos no un estatus jurídico del *hacking,* pero sí facilitar que por estas vías de colaboración podamos plantearnos en un momento dado poder detectar, reparar y solucionar brechas de seguridad que puedan darse en los sistemas informáticos; porque como digo las brechas están. No hay capacidad técnica en España para resolver todos los problemas de seguridad que se van a dar. Lo que ha demostrado la historia de la informática es que hay una evolución constante de lenguajes, de sistemas, de problemas, y aparecen errores informáticos que llevan años e incluso décadas presentes, y que hasta que alguien no se mete a fondo con ellos no lo detecta. Pensar que vamos a programar algo perfecto es imposible. Por lo tanto tenemos que ver cómo permitimos la colaboración de personal civil e incluso la notificación de brechas de seguridad, de problemas de seguridad, sin miedo a determinadas represalias.

Todo esto también tiene que ver con algo que me han trasladado desde instituciones relacionadas con la justicia, en relación con la colaboración entre los organismos del Estado, civiles y militares. Como digo la ciberseguridad, que la podemos enfocar desde la seguridad nacional, no es una especie aislada o que no tenga incidencia en aquellos aspectos más rutinarios o más ordinarios de la vida cotidiana. Militarizar instituciones o militarizar los organismos de coordinación sin permitir la colaboración con el estamento civil —incluso como digo a nivel de instituciones como jueces o fiscales especializados en delincuencia informática— lo único que hace es debilitarnos a todos. Creo que estos mecanismos deberían potenciarse y deberían agilizarse.

Además de todo lo anterior hoy por ejemplo se ha conocido, que es otra cosa que hay que tener en cuenta, un acuerdo del CNI, del Centro Nacional de Inteligencia, con Microsoft para garantizar el acceso al código fuente de aplicaciones de un proveedor informático. Como persona que se preocupa por estos

cve: DSCG-12-CM-102

temas yo llevo muchos años defendiendo la necesidad de incorporar cada vez más el *software* libre o el *softwar*e auditable, el *software* de código abierto o de fuentes abiertas, como lo quieran denominar, en aquellos procesos críticos que permitan una revisión y una mejora, y que no se dependa, y más cuando se trata de infraestructuras críticas o de planes de seguridad nacional o que afecten de manera directa a la seguridad del Estado, de la voluntad de una determinada empresa en querer solucionarlo, en querer arreglarlo, en tener el parche de seguridad disponible en cualquier momento.

No sé si recuerdan el año pasado que hubo una afectación a muchas empresas en España por un virus que se llamaba *WannaCry,* que era un virus que aprovechaba una vulnerabilidad de un sistema determinado, que se propagaba en red y que afectó a muchos programas. Mientras las empresas no quisieron arreglar ese problema ese virus se propagó y no se pudo solucionar de manera completa. Supongo que habrán oído hablar también de los fallos de seguridad incluso a nivel *hardware* en procesadores, en los chips que hacen que funcionen los ordenadores, como Spectre y Meltdown, que son fallos que solo puede ser arreglados por los propios fabricantes de estos procesadores. No es que el ordenador no vaya a funcionar, es que se permitía que el código leyese instrucciones de memoria y que por tanto se pudiera acceder a información confidencial tratada en estos sistemas. Por tanto mi experiencia me dice que debemos apostar más por determinada capacidad técnica para resolver estos problemas, y todo ello debería estar basado, por razones evidentes, en la posibilidad de auditar los códigos informáticos, el *software* del que dependen la mayoría de nuestros sistemas. Como digo, si hay un fallo de seguridad en sus teléfonos móviles que permite a cualquier ajeno a la información que ustedes manejan acceder a esa información, ¿cuánto tiempo va a tardar Apple en solucionarlo si utilizan un dispositivo de Apple? ¿Quién va a solucionarlo? ¿Tienen los servicios del Congreso los mecanismos técnicos para arreglarlo? Son reflexiones que creo que debemos plantear.

Ya para terminar, y agotando el tiempo que tan amablemente me han cedido, me gustaría comentar algo respecto de las criptomonedas, que sin duda es uno de los aspectos que más se relacionan con la potencialidad de realizar actividades ilícitas en Internet y que pueden tener una afectación. Como saben las criptomonedas vienen a ser una evolución del concepto de sistema de pagos o de un sistema fiduciario en el que, entre diferentes partes, se ponen de acuerdo para realizar transacciones y hacer anotaciones en una base de datos, en este caso distribuida. Esto permite el envío de una transacción a una persona, en este caso por ejemplo podría ser en *bitcoins,* que le va a dar un valor. A lo largo de estos meses pasados como digo muchas personas se han puesto en contacto con nosotros para que les ayudáramos a gestionar la posibilidad de abrir un intercambiador, una página web o un lugar físico en el que poder cambiar unas criptomonedas por euros, poder comprar, vender y operar, igual que sucede en otros muchos lugares de Europa. Tenemos el problema de que no es posible trabajar con bancos en España. Hay miedo a relacionarse con estas tecnologías que han llegado para quedarse, que van a significar el futuro. Y lo que ello está provocando es que mucha gente opere con casas de cambio que no están en España, lo que nos sustrae a la posibilidad de control, de información, de regulación, de control fiscal. Frente a novedades tecnológicas como esta no debemos reaccionar con miedo o de forma prohibitiva, yendo más hacia la prohibición, sino que a veces es más inteligente colaborar, cooperar o facilitar, porque de esa forma tenemos mucho más acceso a la información. Desde aquí les invito a que, más que ver esto como un problema para la seguridad, que seguramente tiene sus riesgos y no los vamos a negar —hay aplicaciones que van a dificultar el rastreo o saber quién está detrás de una determinada transacción u operación económica—, sin embargo si lo facilitamos en la mayoría de estas cuestiones, primero, tendremos profesionales que sabrán cómo rastrearlas, cómo localizarlas, segundo, tendremos mucha más información de quién opera con ello en España y con qué fines, y por tanto también tendremos muchas más posibilidades de intervenir y de regularlo.

Creo que he agotado el tiempo que tenía.

El señor **VICEPRESIDENTE:** Muchas gracias por la comparecencia.

Vamos a dar un turno de cinco minutos —dijimos que era un solo turno— comenzando de menor a mayor.

¿Por el Grupo Parlamentario Mixto? **(El señor Yanguas Fernández renuncia).**

Por el Grupo Parlamentario Vasco tiene la palabra el señor Legarda.

El señor **LEGARDA URIARTE:** Muchas gracias, presidente. Muy brevemente.

En primer lugar, quiero agradecer al compareciente su presencia en la Comisión y las explicaciones y sugerencias que nos ha hecho. Respecto a algunas de las cuestiones que ha indicado, que eran

cve: DSCG-12-CM-102

básicamente cuestiones de contenido normativo o aspectos que habría que subsanar mediante el ordenamiento, la primera cuestión que apunta usted es la vinculada al Reglamento de Protección de Datos. Este reglamento como sabe usted no es propiamente una trasposición, pero en los ámbitos que deja el reglamento en esta Cámara se ha constituido una ponencia, y estamos en trámites de aprobación de la ley de protección de datos. La peculiaridad es que como usted sabe en este reglamento europeo se crea el primer derecho fundamental de los ciudadanos de la Unión. Por tanto ha dejado de ser un ámbito a disposición de las legislaciones de los Estados. Directamente por la Unión se crea un derecho fundamental y genera una serie de derechos entre los particulares. El ámbito de actuación de las legislaciones estatales es muy reducido en ese sentido, o solo en aquellos ámbitos que permite, y uno de los ámbitos que no permite es lo que se llama la responsabilidad activa.

Nosotros veníamos de un modelo francés en el que estaban perfectamente estipuladas las obligaciones de las empresas que manejaban datos de ciudadanos, pero este modelo ya no existe en la legislación europea, en el reglamento. Es un ámbito de responsabilidad activa en un modelo más anglosajón que continental, y se basa en el principio de que el que genera un riesgo, en función del riesgo que genera, debe adoptar las medidas para solventarlo. Luego vendrán los delegados, el responsable y las agencias oficiales de protección de datos que, a través de inspecciones, determinarán si cada empresa ha cumplido con esa responsabilidad activa, que es variable en función del riesgo, por los datos que tratan y por su volumen, de las empresas. Por tanto esa sugerencia que nos hacía considero personalmente que va a ser inviable, porque supondría cambiar el modelo del reglamento europeo, y eso no está a disposición de los Estados. Es una cuestión que se ha manifestado recurrentemente por varios ponentes, pero entendemos que no está a disposición esta Cámara ni de ninguna Cámara de los países de la Unión.

Respecto a la investigación de delitos efectivamente la Ley 25/2007 luego fue en cierta medida enmendada por un par de reformas que hubo en el Código Penal, y después en la fase de investigación por la Ley de Enjuiciamiento Criminal; lo que usted sugiere —es una reflexión a ver qué le parece— es la paradoja de los opuestos del mundo de la globalización. El mundo global genera una paradoja y son las respuestas locales. En un mundo global un tema como la ciberdelincuencia no puede ser abordado ya por legislaciones estatales o nacionales, como prefieran llamarlo. De hecho hay un consenso en que debe ser abordado, al menos en nuestro marco regional, por instituciones superiores, tanto el Consejo de Europa como la Comisión. Están también los convenios de Budapest, que persiguen esa criminalidad global, por el problema que usted conoce que hay del concepto de territorialidad, que ha dejado de existir. El derecho penal se basaba en el territorio, porque era una manifestación de la soberanía, pero se ha quebrado ese concepto, y tenemos un problema de identificación y de atribución de los delitos, que solo va a poder ser solventado por normativa internacional, en nuestro caso de nuestro ámbito regional, que es tanto el Consejo como la Directiva NIS para la seguridad de los equipos y los acuerdos de Budapest. Por cierto, uno de los protocolos no lo tiene todavía ratificado el Estado español.

Respecto al *hacktivismo* a LexNET las noticias que yo tengo dicen que la imputación que se hace es porque hubo una suplantación de identidad, no solo hubo una dación de cuentas de que había una brecha en el sistema, sino que realmente hubo una suplantación de identidad, que es por lo que está imputada esa persona, al menos por las explicaciones que nos dio aquí la fiscalía.

Respecto al intercambiador me remito a lo que he comentado de que no puede haber una respuesta local a un problema global, porque entonces las diferencias de los acercamientos locales generan las disfunciones que generan y a su vez otras brechas. Creo que lo que usted comentaba de los intercambiadores de métodos de cambio oficiales a métodos de cambio que funcionan, pero que no son oficiales, también debiera ser regulado no de una manera local, como me ha parecido entender que sugería, sino desde una aproximación de una regulación global, en nuestro caso regional, de la Unión o del Consejo de Europa. Simplemente le hago estas reflexiones a efectos de su valoración.

Quiero agradecerle de nuevo su intervención y lo interesante que ha sido su exposición. Muchas gracias.

El señor **VICEPRESIDENTE:** Muchísimas gracias, señor Legarda.

Tiene la palabra el señor Gutiérrez por parte del Grupo Parlamentario Ciudadanos.

El señor **GUTIÉRREZ VIVAS:** Gracias, señor presidente.

Gracias, señor Maeztu. Me uno a las palabras de mi compañero, el señor Legarda, y le doy la bienvenida a esta Comisión y a esta casa que, como bien conoce, también es la suya.

cve: DSCG-12-CM-102

Yo estoy bastante de acuerdo con lo que ha dicho el señor Legarda sobre la responsabilidad activa de las empresas. Evidentemente, ese es el sentido del que emanan las nuevas directivas europeas y, por tanto, quizás el punto de encuentro. Yo quería comentarle dos cosas relacionadas con esto. Una, que usted ha mencionado, sobre el código abierto de los fabricantes que, al final, es un debate que ha estado en el mundo de la tecnología desde siempre y que ha existido desde que existe el *software.* Yo lo que creo —y le pregunto cuál es su opinión— es que las legislaciones deberían ser un poco más exigentes con los fabricantes. Para mí no se trata tanto de si el código es abierto o de si el propio fabricante conserva los derechos, porque a fin de cuentas ha invertido también tiempo y trabajo de profesionales para desarrollarlo, sino de que tiene que tener una responsabilidad sobre lo que hace ese *software.* Estamos hablando de un mundo conectado totalmente y con unas vulnerabilidades que son crecientes. Básicamente, las vulnerabilidades del *software* de los fabricantes obedecen a que el fabricante hace ya muchísimos años que ha dejado de hacer un control de calidad sobre su producto y deja que el usuario sea el que haga el control de calidad. Se ahorra los controles de calidad y el usuario hace el suyo, demandando si algo no funciona, si tiene una brecha, si tiene una vulnerabilidad; saca su parche, hace una actualización continua. Lo sufrimos todos los que estamos viendo actualizaciones continuas de los dispositivos cada dos por tres.

Eso obedece, simplemente, a que el fabricante se ahorra gran parte de lo que antes sí se hacía, un control de calidad eficiente de su producto. Ahora ha dejado que sea el usuario quien lo haga. Yo creo que habría que obligar más a los fabricantes a que ejercieran un control de calidad adecuado y, sobre todo, a que tuvieran las sanciones adecuadas cuando esto no funcione, porque al final es obligación suya, sobre todo cuando ese *software* al final es de su propiedad. Lo digo porque el Internet de las cosas, que está aquí, que está encima, va a hacer que todavía haya muchísimos más millones de dispositivos conectados; dispositivos que uno va a tener en su domicilio, en su casa, donde va a haber costumbres, hábitos de uso de los electrodomésticos que estamos utilizando y que van a ser capaces de dar un perfil del usuario, que es lo que al final estamos intentando proteger con la Ley de Protección de Datos y las directivas europeas. Por tanto, sin la implicación directa de los fabricantes, yo veo que es realmente complicado que esto se solucione.

En segundo lugar, le quería poner algo en discusión. Usted decía que no hay que hacer un estatus del *hacking.* Yo no estoy muy de acuerdo, yo creo que se debe hacer un estatus del *hacking* ético. Creo que es algo que las empresas utilizan cada vez más y, evidentemente, eso significa detectar vulnerabilidades de sistemas propios pero también de otros sistemas, y debe haber un cierto estatus como hay un estatus de la protección del denunciante —al menos es algo que estamos intentando hacer en esta Cámara—. Al final, no deja de ser denunciar de una manera, no algo que es ilegal, pero sí algo que desde el punto de vista de la competencia y de la seguridad de los usuarios está quebrando ese principio de confianza en el fabricante. Por eso quería saber su opinión porque quizá deberíamos hacer una legislación sobre el *hacking* ético.

Muchas gracias. Le reitero nuestro agradecimiento por su comparecencia.

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

Por el Grupo Confederal de Unidos Podemos-En Comú Podem-En Marea, el señor Comorera tiene la palabra.

El señor **COMORERA ESTARELLAS:** Muchas gracias, señor presidente. Muchas gracias por su comparecencia, señor Maeztu. Me uno a lo manifestado por mis compañeros.

En relación con la ciberseguridad, es interesante para esta Comisión conocer un punto de vista diferente —como sería desde la abogacía, por ejemplo— de los puntos de vista que hemos tenido hasta ahora. Nuestro grupo cree que en materia de ciberseguridad debe haber, y no puede faltar nunca, un elemento principal que no es otro que la salvaguarda de derechos fundamentales, sin atacar la privacidad y la confianza entre Estados, que son los únicos pilares que pueden sustentar una estrategia creíble en materia de ciberseguridad. Así lo defiende, por ejemplo, el Supervisor Europeo de Protección de Datos, que alerta sobre las deficiencias de la estrategia de la Unión Europea en esta materia y llama la atención para que la seguridad informática no se convierta en una excusa para controlar ilimitadamente la información personal de los ciudadanos. Sé que es un pregunta difícil, pero ¿cómo cree usted que podemos garantizar que en el uso de las TIC se proteja el derecho a la intimidad y el derecho a saber quién tiene nuestros datos personales, cómo se ha accedido a ellos, para qué se utilizan y posibilitar su control y cancelación? Un caso que ha saltado hace poco a los medios es el del conocido como la 'App de la Liga' —supongo que habrá oído sobre él— y me gustaría conocer su opinión al respecto.

cve: DSCG-12-CM-102

En un artículo que publicó usted llamado *Buenas prácticas en el tratamiento de medios de prueba digitales,* en 2015, señalaba que respecto al impulso digital se requería una inversión en infraestructuras TIC, como el *cloud computing* y el *big data,* la investigación e innovación para impulsar la competitividad industrial y una sociedad que cuente con mejores servicios públicos y mejores habilidades digitales para los ciudadanos. Aplaudía la iniciativa de la Comisión Europea en el sentido de intentar plantar cara a Estados Unidos y posicionarse como un referente mundial en la economía digital, pero era escéptico. Esto era en 2015; le quería preguntar si sigue siendo usted tan escéptico.

Como ya ha comentado usted, la cooperación entre el sector público y el privado en el intercambio de información he entendido que usted la considera insuficiente. ¿Qué cree que deberíamos hacer desde el Poder Legislativo para potenciar esa cooperación? Asimismo, ¿de qué manera considera que se debe abordar desde la Administración la creciente expansión del llamado Internet de las cosas, dadas las implicaciones que puede tener para las infraestructuras críticas? En cuanto a la inversión —es una pregunta que acostumbro a realizar a todos los comparecientes—, y más si nos comparamos con otros países como Reino Unido o Estados Unidos, ¿usted cree que tenemos un problema grave por la falta de inversión en ciberseguridad?

También quería hablar sobre la propuesta de Directiva europea de derechos de autor, teniendo en cuenta que usted es especialista en propiedad intelectual, sobre todo de los problemáticos artículos 11 y 13 en relación con posibles vulneraciones de derechos. Nos preocupa que un algoritmo acabe haciendo lo que debería estar reservado para un juez y que la normativa de derechos de autor acabe siendo como un banco de pruebas para otros recortes de derechos. Me gustaría conocer cuál es su opinión al respecto y cuál cree que debería ser la posición del Gobierno español en relación con estos artículos.

Por otra parte, se va lanzando cada cierto tiempo como globos sonda la prohibición del anonimato en las redes sociales. Me gustaría también conocer su opinión al respecto teniendo en cuenta que el anonimato está reconocido por Naciones Unidas y que ya existen métodos para averiguar identidades, eso sí, siempre ordenado por un juez o un tribunal. ¿Cree usted, por tanto, que el anonimato pudiera estar en peligro?

Y, para acabar, me gustaría preguntarle su opinión, porque usted ha sacado la cuestión de LexNet, sobre si LexNet debería continuar en manos del Ministerio de Justicia o tendría más sentido que LexNet estuviera en manos del Consejo General del Poder Judicial.

Muchas gracias, de nuevo, por su interesante comparecencia.

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

Tiene la palabra en representación del Grupo Socialista el señor Luena.

El señor **LUENA LÓPEZ:** Gracias, señor presidente.

Gracias, señor Maeztu, por sus palabras. Enhorabuena, paisano, por la exposición y gracias también porque nos ha desvelado en su intervención que les piden a veces que ayuden para detectar fallos de seguridad, brechas de seguridad —creo que ha dicho usted—. Desde la Cámara Baja, desde el Congreso, desde el Senado y desde esta Comisión mixta le agradecemos esa colaboración.

Le voy a hacer una pregunta sobre un tema que otros portavoces ya han desgranado e igual me repito, pero seré breve, y le pido disculpas de antemano. Hemos estado hablando de la directiva, el compañero de Podemos hablaba ahora del reglamento de datos y usted de la seguridad de los datos, por lo que querría saber su percepción, porque lleva muchos años en ejercicio, sobre el grado de concienciación del riesgo que hay en la red o, dicho de otra forma, sobre si usted cree que hay un grado de concienciación alto, medio o bajo acerca de la fragilidad de la privacidad de los datos, por decirlo casi de una forma eufemística.

Usted es un experto en derecho y le vamos a pedir ayuda. Le habrán informado desde la Mesa que esta Comisión y esta ponencia tienen el sentido de ayudar a la seguridad nacional a mejorar en la ciberseguridad. Por eso, según usted, ¿qué legislación actual necesitaría una actualización más urgente y que se pueda hacer de manera inmediata cuando esta Comisión concluya su ponencia? ¿Cree usted que es necesario tipificar con más detalle en el Código Penal los delitos cibernéticos? Si es así, me gustaría que nos indicara cuales serían para usted los prioritarios.

Aunque el señor Legarda ya le ha preguntado al respecto, ¿cree necesaria la existencia de una carta específica de derechos y deberes digitales y, sobre todo, como ha dicho el señor Legarda, en qué ámbito? ¿En el nacional, en el europeo? ¿Con qué rango? ¿Con modificación de leyes e incluso con un futura reforma constitucional? Nos ha hablado usted sobre el esquema nacional de seguridad, pero me gustaría

cve: DSCG-12-CM-102

que nos concretase una cuestión. ¿Cree necesario que se actualice para darle, desde el punto de vista de la ciberseguridad, mayor alcance, por ejemplo, con empresas de servicios públicos con infraestructuras críticas, como decía usted al principio? ¿Cómo regularía usted —y alguna cosa ha dicho, pero me gustaría que concretase más— la figura de los cibervoluntarios entendidos como *hackers* que ayudan en la defensa de la ciberseguridad del país? Para finalizar con esta parte, ¿dónde fijaría la frontera legal entre el ciberactivismo y la ciberdelincuencia? Porque son campos que necesitan de un afinamiento jurídico mayor. ¿Le parece que los mecanismos de control que existen ahora son suficientes para que se puedan detectar esas diferencias?

Termino con una pregunta de carácter local. Usted ha hablado de LexNET y ha puesto un ejemplo sobre nuestros propios dispositivos en esta Cámara, en el Congreso los Diputados, pero quiero preguntarle por los ayuntamientos —una institución que usted conoce muy bien, me consta— porque las administraciones locales almacenan datos que son muy sensibles para los vecinos: padrón, censo, domiciliación de cobros de impuestos, etcétera. ¿Están preparadas las administraciones locales españolas contra los ciberataques? Como esto es público, díganos que sí, pero díganos las deficiencias, los problemas que tienen los ayuntamientos. En ese sentido, casi prefiero que me responda más a la segunda pregunta. ¿Qué recomendaciones de ciberseguridad realizaría a las administraciones locales y, por supuesto también, a las instituciones nacionales para que les ayuden en el asunto que nos ocupa?

Le reitero el agradecimiento porque es muy importante que a esta Comisión mixta se acerquen personas como usted para ayudarnos en una tarea que es muy importante y en la que estamos volcados en esta Comisión.

El señor **VICEPRESIDENTE:** Muchísimas gracias, señor Luena.

Para finalizar con la ronda de intervenciones de los grupos parlamentarios, tiene la palabra la señora Moro en representación del Grupo Popular.

La señora **MORO ALMARAZ:** Muchas gracias, señor presidente.

Buenos días, señor Maeztu. Al igual que quienes me han precedido en el uso de la palabra, quiero agradecerle su comparecencia y tener la oportunidad de escucharle y compartir aquí, en sede parlamentaria, muchas de sus inquietudes y también de sus conocimientos.

Es evidente que usted nos ha planteado muy diversas cuestiones que merecerían muchísimo desarrollo, pero tenemos el tiempo que tenemos. Usted forma parte de una época y de una serie de profesionales que prácticamente nacieron con la ebullición de un Internet un poco más avanzado y de las nuevas tecnologías y sabe, como yo, que la filosofía que en este entusiasmo de un crecimiento tan importante y tan rápido de una nueva tecnología, de instrumentos de comunicación, de instrumentos de formación, fue entender por algunos, no por todos, Internet como un mundo sin fronteras, como una especie de ciudad sin ley, luego extendido a las tecnologías de las aplicaciones en el ámbito de la información y la comunicación. Era, además, algo muy atractivo donde el joven podría desarrollar toda su creatividad, que era la huida del mundo analógico, una especie de huida del mundo real, lo que evidentemente era atractivo en un mundo conflictivo. De ahí el anonimato, de ahí la defensa a ultranza de la gratuidad, de ahí la defensa a ultranza de la libertad por encima de las normas, pero Internet y las aplicaciones informáticas son otra cosa. Tenemos también la filosofía, que alguna gran empresa hizo suya, de que en este mundo digital, del ciber, nada es imposible y, por tanto, si nada es imposible, todo aquello que sea posible hay que realizarlo y realizado, se superpone al mundo de la seguridad, de la norma y de la ley.

En consecuencia, nos resulta muy complicado navegar cuando todavía vamos pensando desde la perspectiva de la seguridad y en las normas en un mundo analógico, lento y seguro que abarcamos frente a este mundo que, como han dicho aquí mis compañeros anteriormente, se va de las fronteras, no tiene puertas, no tiene ventanas, algo que queremos atajar con instrumentos que en absoluto están adaptados para ello. Por lo tanto, muchas de esas cuestiones que en esta Comisión tienen que atarse de alguna forma para tener las ideas un poco más claras parten de que hemos estado navegando con eso y que, por tanto, las propias normas han sido parches y se han quedado obsoletas simplemente en el momento de incorporarse, por tanto, es muy difícil afrontarlo desde espacios locales, desde espacios nacionales. Por esa razón sería muy difícil que yo le preguntara mucho más al respecto, pero sí me gustaría que detallara algo más sobre cuál es su filosofía en este momento, cuando ya hemos pasado otras etapas, a la hora de enfocar las regulaciones, no una regulación concreta, aunque usted ya nos ha planteado algunos problemas y se le ha preguntado al respecto.

cve: DSCG-12-CM-102

Usted conoce cómo enfocamos en muchos casos la idea de la neutralidad tecnológica a la hora de regular, pero es que en este momento nos encontramos con un paso más. Yo quiero utilizar una frase suya de un artículo sobre un tema que le ocupa y que es interesantísimo en este momento. Usted dice: Toda la tecnología que hace funcionar el *bitcoin* es muy valiosa y lo será cada vez más en el futuro. Me gustaría que nos desarrollara más esto porque lo he entendido en el sentido de que no solo es importante debatir sobre el *bitcoin* y sus problemas o ventajas, sino sobre la tecnología que está detrás y cuyas aplicaciones y resultados pueden ser muy distintos y muy rápidos. Los drones eran una cosa, sin embargo, la tecnología dron es lo que nos está llevando a otras aplicaciones, que son las que en un momento determinado también pueden afectar sin duda a la seguridad nacional.

Por esa razón quiero insistir un poco más sobre algo que usted ha planteado en el tema de los códigos abiertos. Esto ha sido también toda una filosofía que ha aparecido en el momento de aprender a vivir en el mundo digital, pero cuando hablamos de aplicaciones o infraestructuras críticas, me gustaría conocer un poco más sobre cuál es la ventaja, según usted, de ese código abierto. Ustedes han estado luchando mucho por el código abierto en cuanto a las aplicaciones en justicia y quizá eso también haya llevado a que se haya visto LexNET como algo a lo que batir porque no se correspondía con la idea de un código abierto en la base. Confundir ambas cosas no nos permite avanzar. Creo que hay que ser críticos y autocríticos y conocer bien cuáles son las deficiencias, sobre todo en materia de infraestructuras críticas —lo estoy diciendo de manera incorrecta, pero usted me está entendiendo— y de seguridad nacional porque, indudablemente, el confiar en aplicaciones de empresas diseñadas por empresas con un determinado modelo tiene sus problemas, pero también ir a otras filosofías si no tenemos suficientes garantías en determinados ámbitos es extremadamente complicado.

No es por lo que usted ha dicho, sino por lo que he oído de alguno de mis compañeros. Quiero dejar claro —algo ha dicho el señor Legarda— que en el tema de LexNET se ha creado después mucha filosofía política para atacar algo que, efectivamente, nos tenemos que tomar en serio. El Gobierno se lo tomó en serio y, sin embargo, no produjo un acceso a aquello que algunos están defendiendo y por lo que plantean que sea el Consejo General del Poder Judicial o el Gobierno el que se ocupe de un tema cuya competencia en estos momentos corresponde, sea cual sea el signo del Gobierno, al Ministerio de Justicia.

Concluyo. En relación con este tema —aunque este solo es un ejemplo—, está el papel de los *hackers*. A mí sí me parece que hay que incorporar esta cuestión a ese salto de la filosofía de la legislación pasada a una legislación que tiene que afrontar los problemas del presente y, sobre todo, del futuro. Por tanto, habrá que definir términos y conceptos distintos porque, indudablemente, no creo que sea lo mismo la concepción que tenemos del *hacker* como alguien que ataca que la concepción de alguien que prueba, de alguien que constata brechas de seguridad. Por tanto, creo que puede ser una buena filosofía favorecer y aclarar cuáles son los ámbitos y las denominaciones incluso, para quitar ese halo perverso de aquel que ataca y, por tanto, viola derechos y suplanta identidades y, por tanto, transmite a otros que tienen la obligación como abogados de mantener obligaciones respecto a su cliente, respecto a la ley, etcétera. Yo sí creo que hay que regular, pero con la mentalidad del ámbito de lo digital. Pongo encima de la mesa esto de cambiar el nombre porque, efectivamente, las obligaciones y las responsabilidades de alguien que ayuda, de alguien que aporta deben quedar perfectamente diferenciadas de las de aquel que investiga pero ataca.

Muchas gracias.

El señor **VICEPRESIDENTE:** Muchas gracias.

Habiendo acabado la única intervención de los grupos parlamentarios, le doy la palabra al compareciente.

El señor **MAEZTU LACALLE** (Abogado especializado en Internet, propiedad intelectual y tecnología): ¿Tengo que llevar algún orden?

El señor **VICEPRESIDENTE:** Con libertad.

El señor **MAEZTU LACALLE** (Abogado especializado en Internet, propiedad intelectual y tecnología): Lo digo por el tiempo, porque han salido muchas cuestiones. Voy a intentar agrupar las más recurrentes, y discúlpenme si hay alguna cuestión que no pueda atender.

cve: DSCG-12-CM-102

Respecto al Reglamento General de Protección de Datos, sobre lo que ha habido varios planteamientos, evidentemente, conozco el contenido del reglamento, conozco el tema de la responsabilidad activa, pero eso no quiere decir que no tengamos que ingeniarnos mecanismos que son recomendables para que una pequeña empresa que no tiene los recursos de Facebook o de otras empresas sepa exactamente qué medidas ha de adoptar, porque eso va a ayudar no solo a proteger los datos personales, sino a proteger las estructuras y los sistemas. Si esta aplicación de rastreo de deporte no publica datos personales, sino que publica las rutas, en el fondo está afectando. Que empresas pequeñas tengan claras cuáles son las obligaciones que tienen que asumir y no haya una indeterminación de adoptar aquellas que sean más convenientes, como han proporcionado, es importante y creo que debemos hacer un esfuerzo, ya sea a través de la Agencia de Protección de Datos, ya sea a través de las guías, a través de resoluciones o a través de instrumentos que seguro que podemos encontrar. Además, como ha manifestado, si no soy el único al que se le ha ocurrido plantearlo, supongo que los que estamos trabajando en el otro lado de la barrera vemos que hay algún tipo de problema. Efectivamente, no podemos regular cualquier cosa. La ley orgánica que se está tramitando tiene el alcance que tiene y puede llegar a lo que puede llegar, y eso es absolutamente innegable.

Salto un poco y paso a comentar el tema de LexNET, sobre el que se me han planteado varias cuestiones. Voy a exponer un poco mi opinión. Lo que sucedió con LexNET, con independencia del contenido concreto de lo que pueden ser actuaciones judiciales o no, era que se desplegó una versión de funcionamiento que dejaba un campo en la barra de direcciones que tenía el identificador de usuario. Yo, por naturaleza y sin pretender hacer nada, siempre que veo una web que me marca un identificador de usuario cambio el número que me pone al final, y no porque pretenda entrar en la cuenta de nadie, sino para ver qué pasa. Es un problema que tengo yo y lo hago. Lo que sucedía es que, como no tapaban esa dirección, se podía acceder a los buzones de otros compañeros abogados. Esto, que es lo que se denunció y se puso de manifiesto en su momento, con independencia de la persona acusada, es lo que ha generado problemas, incluso se anunció que se iban a dirigir actuaciones de denuncia contra colegiados que habían realizado eso mismo, no por una voluntad. De hecho, yo hice eso, yo intenté entrar en el buzón de un tercero, no sé de quién. Yo cambié ese número porque mi decano me pidió que le explicase qué había pasado y si estaba ya arreglado. Por eso yo lo hice, y cuando el Ministro de Justicia salió en su momento diciendo que había cuarenta y nueve pensé que uno debí ser yo porque yo lo hice. Y, sin embargo, a mí no me habían detectado porque luego me dijeron que yo no estaba en la lista. Es decir, que el sistema tampoco detecta quién intenta acceder y quién no. Por tanto, hay un problema de seguridad.

Anécdotas aparte, lo relevante es lo siguiente. Quiero que piensen ustedes si yo fuese consejero de Justicia de una comunidad autónoma, que es quien dota de ordenadores a los jueces y fiscales, porque el Poder Judicial no compra los ordenadores; los compran las comunidades autónomas, que tienen cedidas las competencias, como en mi caso, por ejemplo, La Rioja. Si yo fuese consejero de Justicia de La Rioja, podría decidir que los ordenadores que comprara a mis jueces llevasen un *software* determinado que me informase de todo aquello que los jueces teclearan en ese ordenador. ¿Quién sabe qué tiene ahí? ¿Por qué un consejero puede decidir hacer eso? Porque yo podría hacerlo, le encargo al proveedor que instale unas determinadas aplicaciones, y nadie lo controla. Se dice que el que pone los medios es el Ejecutivo. Al Poder Judicial se le puede dar el dinero para que compre los ordenadores para los jueces, para que todos los jueces tengan los mismos ordenadores, los mismos equipos y haya una garantía de que lo que se utiliza no esté infiltrado por ningún de otro poder. Y esa es la crítica que hacemos, los sistemas informáticos no son máquinas de escribir; a veces pensamos en un esquema de hace veinte o treinta años, pero hoy en día un ordenador es mucho más que una máquina de escribir y no sirve solo para escribir la sentencia, sino que puede dar mucha información. Los sistemas informáticos, con la potencialidad que tienen ahora, permiten, por ejemplo, sin necesidad ni tan siquiera de acceder a lo que teclea el juez, que yo pueda, a través de un sistema informático determinado que gestiona las notificaciones judiciales, saber qué abogados llevan qué empresas, saber cuándo se presenta una demanda, saber cuándo se contesta una demanda; podría tener muchísima información. Simplemente son metadatos, ni siquiera necesitaría acceder a mucha información sobre el procedimiento judicial, pero me podría dar un poder muy relevante sobre la actuación que se desarrolla en el ámbito de otro poder del Estado.

Por eso cuando se me ha preguntado cuál es mi opinión sobre por qué LexNET debe estar controlada por el Consejo General del Poder Judicial es porque entendemos que es una herramienta que tiene una potencialidad de intrusión en un poder que la propia separación de poderes recomienda mantener

cve: DSCG-12-CM-102

separados. Por tanto, creo que no debería ponerse en cuestión. Creo que con ello he contestado a lo que me planteaba el señor Comorera sobre esta cuestión.

Respecto de los *hackers,* la idea general que me llevo, para mi grata impresión, es que todos ustedes entienden el *hacking* positivo o desde un contexto mucho más positivo y más útil para la seguridad, para la defensa de todos de lo que hasta ahora se había venido transmitiendo, y me alegro que eso sea así y que, por lo tanto, pueda tener sentido, como plantean, que se desarrolle un estatuto de colaboración informática o del ciberactivista o cibervoluntario —como lo queramos llamar—, en el sentido de dotar de seguridad jurídica para aquel que, sin ánimo de dañar, sino simplemente de mejorar o ayudar, tenga la seguridad de que no va a haber represalias por el hecho de comunicar un fallo o una incidencia de seguridad. Eso sí que creo que es una medida positiva. Creo haber percibido en los grupos que han intervenido que habría una disposición positiva en ese sentido, de lo cual me congratulo porque mucha gente cuando viene a preguntarnos qué hacer cuando han descubierto fallos de seguridad lo hacen precisamente porque no tienen la certeza de que no vaya a tener consecuencias negativas, aunque no hayan pretendido hacer nada, sino que lo hayan descubierto porque han utilizado un buscador que busca fallos de seguridad, porque han rastreado una serie de direcciones IP que había recibido algún tipo de ataques en sus propios sistemas, etcétera.

Otra cuestión que se ha reiterado es en relación con el *software* de código abierto. Aquí debemos distinguir —y tiene que ver también con otra cosa planteada—, por un lado, la aplicación de *software* de código abierto o la aplicación de *software* propio en sistemas críticos o en aquellos instrumentos que puedan tener una mayor afectación para la seguridad nacional. Esto lo que provoca es no depender de un tercer proveedor o de un tercer país con intereses que pueden ser divergentes en un momento determinado. En un principio es previsible y normal que las relaciones con Estados Unidos sean buenas y normales y que no haya problemas que nos indiquen a pensar lo contrario, pero en un momento dado si una empresa de Estados Unidos tiene que servir a su país o tiene que servir a los intereses de España, seguramente sirva primero a los intereses de su país por una razón muy sencilla, porque es donde les pueden sancionar, donde les pueden encarcelar o donde pueden adoptar medidas coercitivas de manera directa. Por tanto, confiar en que un proveedor va a arreglarnos un problema que podamos tener nosotros aquí cuando va a estar sometido a otra normativa es una cuestión que debe invitarnos a la reflexión.

En segundo lugar, la capacidad de formar personal propio que resuelva estos problemas a partir del análisis del código informático es una de las ventajas evidentes que nosotros al menos, la gente que creemos en el *software* libre, vemos como evidente para un país. ¿La capacidad de desarrollar técnicos competentes de primer nivel? Ya los hay. España es uno de los países donde, no sé si por nuestro talento o por nuestra necesidad constante de buscarnos las habichuelas, más talento informático tenemos, y así lo acreditan muchas pruebas por el mundo. Por lo tanto, tener un campo de desarrollo, poder generar una industria del *software*, poder generar puestos de trabajo, poder estimular el desarrollo de este tipo de cuestiones también es una de las razones que aconsejan en la medida de lo posible que aquellos elementos esenciales para el Estado debamos hacerlos residir al menos en parte en *software* que se pueda auditar, que se pueda mejorar, que se pueda crear. Esto por un lado.

Por otro lado, se planteaba qué hacemos con los datos personales, con las aplicaciones que instalamos. Igual tenemos que establecer sistemas adicionales, garantías adicionales, requisitos adicionales para los desarrolladores, empezando por la posibilidad de auditar el código informático. En la Ley Orgánica de Protección de Datos, el artículo 13, que también está recogido en el reglamento, prevé un derecho que no se utilizaba mucho, que es la impugnación de valoraciones; es decir, que una persona, cuando es sometida a una valoración de sus datos personales por un sistema automatizado, pueda impugnar esa valoración. Es decir, si a mí me van a dar un crédito en función de lo que diga un algoritmo, que yo pueda impugnarlo. Ahora bien, ¿cómo podemos saber cómo funciona ese algoritmo? Haciendo el algoritmo. ¿Cómo podemos saber que lo que nos dicen de la aplicación que ha salido aquí de la Liga realmente hace eso o no lo hace? ¿Por qué nos hemos enterado? Porque lo han puesto de buena fe en sus condiciones de uso, pero si yo no puedo auditar el código informático de una aplicación, yo no puedo saber si la aplicación de la linterna que me he descargado en el teléfono para entrar al trastero porque no tengo luz además me está cogiendo la base de datos de contactos que tengo en el teléfono. ¿Cómo puedo saber eso? Debo tener muy claro que tengo la capacidad de exigirle a las empresas que pueda auditar el código de las aplicaciones que ponen a disposición de los consumidores. Creo que esta es una cuestión esencial. No digo obligar a que sea de código abierto, pero sí que deban estar dispuestos a someterse a una normativa nacional que nos dé a los ciudadanos el derecho a poder auditar qué es

cve: DSCG-12-CM-102

exactamente lo que hace esa aplicación. Tenemos, como digo, teléfonos que hacen de todo y que no sabemos en la mayoría de los casos lo que hacen. Es continúa la información sobre filtrados de datos de muchas aplicaciones; cada vez es más frecuente encontrar en Twitter gente que se queja de que de ha tenido una conversación con otra persona y le ha aparecido publicidad relacionada con esa conversación. Yo les puedo contar que a mí me pasó con un anuncio del Colegio de Abogados de Madrid. Yo estaba en un ascensor con dos compañeros de aquí, de Madrid —yo estoy colegiado en La Rioja—, estaban hablando sobre las elecciones del Colegio de Abogados de Madrid y en mi teléfono al día siguiente me apareció publicidad sobre las elecciones del Colegio de Abogados de Madrid. Esta es una cosa que, sin haber buscado información, a uno le sorprende. ¿Será casualidad porque saben que soy abogado? No lo sé, pero son cosas que empiezan a asustar y que, como digo, cada vez son más frecuentes. ¿Sabemos lo que hacen las aplicaciones? No, y yo creo que deberíamos ir en ese sentido.

Se han planteado por parte del PNV cuestiones relacionadas con la territorialidad, la Ley 25/2007, y creo que en el fondo son problemas que nos afectan a todos. Efectivamente, yo abogo no por que no se analice el problema, sino porque cuando hay una resolución judicial como la del tribunal de justicia en su momento, la reacción que yo he vivido desde el regulador en España, la reacción de fiscales y de jueces, ha sido negar la evidencia de lo que la sentencia del tribunal de justicia decía. Al final nos está pasando que se anula una norma y tenemos un montón de procedimientos judiciales abiertos donde hemos cogido a los malos e igual los tenemos que soltar porque nos hemos quedado sin norma que ampare una determinada intromisión en derechos fundamentales. A veces somos muy, digamos, autocomplacientes —esto ya lo resolveremos— y nos olvidamos de que hay un tribunal superior que a veces nos anula este tipo de cuestiones. Quiero recordarles un asunto que a mí me produjo bastante indignación. Fue el registro de un ordenador por parte de unos agentes de Policía Nacional en una tienda de Sevilla sin orden judicial. El registro de ese ordenador —donde se encontró pornografía infantil, en una tienda de ordenadores de Sevilla— fue validado por el Juzgado de lo Penal de Sevilla, por la Audiencia Provincial de Sevilla, por el Tribunal Supremo y por el Tribunal Constitucional. El Tribunal Europeo de Derechos Humanos ha tumbado eso porque decía que no había ninguna razón para no haber esperado a la orden de registro del ordenador. Al final se ha tumbado una resolución por parte del Tribunal de Derechos Humanos. Cuando es una cosa tan evidente, como era este caso, debemos evitar que sucedan este tipo de cosas. Debemos tener una normativa y una legislación clara en ese sentido.

Se planteaba también respecto de los *bitcoin* cuál es el problema. El problema es que en Estonia no hay ningún problema, el problema es que en Alemania no hay ningún problema. Es decir, ¿tenemos que actuar globalmente? Evidentemente. Nada de todo lo que yo he planteado tiene sentido desde la localidad. El negarnos a esa evidencia o el actuar de manera timorata como me consta que se está haciendo aquí, creo que no resuelve el problema.

Se me preguntaba por el Grupo Parlamentario de Ciudadanos también, y creo que lo he contestado, pero por concretar, en relación a Leotec, creo que también es aplicable la misma solución. Es decir, yo tengo que saber qué hace mi cacharro, si yo pongo un cacharro en casa tengo que poder saber qué es lo que hace. Y si alguien no está dispuesto a que en un momento dado, por orden de un juez o en un procedimiento de consumo, se pueda analizar qué es lo que hace ese cacharro, no debería poder venderse en España, punto.

Hay un montón de cosas que mi convecino riojano me ha planteado. Quiero citar una en concreto en relación a la reforma de la Constitución española. Mi artículo favorito es el 18.4. Me parece de una inteligencia brutal que en el año 1978 el legislador constituyente español dijera: la ley limitará el uso de la informática. Me parece una brillantez de pensamiento brutal. Cualquier reforma de la Constitución que no toque eso casi me parecerá bien porque lo que me da miedo es que haya una reforma de la Constitución española y se toque eso, ese es el miedo que tengo, que no se perciba la importancia de esa limitación de la informática, ese miedo que había en el año 1978. Cuando uno analiza y estudia las intervenciones parlamentarias en relación a ese artículo, ve que acertaban plenamente en el mundo que describían y que estamos viviendo. Por lo tanto, seguro que hay que reforzar muchos derechos fundamentales, pero hay que arrancar por ese punto. Seguramente también por el derecho al secreto de las comunicaciones. Según el artículo 18, el secreto de las comunicaciones solo se puede levantar mediante resolución judicial; sin embargo, estamos mandando correos, utilizando proveedores de servicios de correo que nos ponen anuncios, con independencia de quién sea el destinatario, que están leyendo esos correos. Ahí tenemos una serie de problemas. Además hay una discusión entre la Sala de lo Social y la Sala de lo Penal del Tribunal Supremo en relación con estos temas que daría para otra intervención muy interesante.

cve: DSCG-12-CM-102

¿La percepción que tengo sobre el grado de concienciación del riesgo en la red? Para mí, alta; para la mayoría de la gente que conozco, ninguna. Yo he nacido en una casa en la que mis padres le tenían un miedo atroz al ordenador porque pensaban que se podía romper; comprar un ordenador era un problema porque no se podía comprar más de un ordenador y, sin embargo, ahora con más de sesenta años usan wasap de manera perfecta, o sea, no era un problema del ordenador. Sin embargo, no saben absolutamente nada de lo que las empresas hacen con todo eso, ni qué uso se va a hacer. Tampoco los padres con los hijos: se están subiendo fotos, se están compartiendo fotos de toda la historia de los menores, que no han tenido la capacidad de decidir si quieren que su vida, desde que tienen meses de edad, en el futuro esté perfectamente rastreada e identificada por empresas. Creo que no hay ningún tipo de responsabilidad y que nadie se lee los términos y condiciones —evidentemente— de las aplicaciones; creo que pocos aquí habremos leído alguna vez de manera completa cuáles son los términos y condiciones de las aplicaciones. Aceptamos todo y luego nos asustamos. Seguramente es necesario algún mecanismo de coordinación de consumo en relación a la nulidad de cláusulas abusivas. Tenemos una Ley de condiciones generales de la contratación que sin duda debe servir para frenar determinados abusos.

¿Legislación con actualización más urgente? ¿Qué hay que cambiar en el Código Penal? Esto sí me daría para una intervención que sin duda sería larga. Si su señoría lo permite, se la puedo hacer llegar por escrito para que la pueda utilizar, así acortaríamos mucho el tiempo de intervención.

¿Actualizar el esquema de seguridad nacional, los cibervoluntarios? Sí, pero las propuestas hay que hacerlas desde el rigor y la seriedad. A veces, cuando se transmite que se va a hacer una ciberreserva, sin pagar, aquello suena a veces a un poco a chiste. Y esto lo que hace es que iniciativas que seguramente tienen buena voluntad o buen fondo acaben un poco diluidas —digamos— ante lo que uno no se puede tomar en serio en una cuestión como la ciberseguridad si se basa simplemente en la mera voluntad de que alguien en un momento dado pueda ayudar o pueda no ayudar, creo que hay que trabajar este tema en serio. Hay mucha gente dispuesta a colaborar, como digo, desde el ámbito civil, y a veces una excesiva militarización de este ámbito puede dar al traste con esas posibilidades de colaboración, y ya digo que no solo de gente como yo, que puede no tener ningún tipo de relación con el Estado, sino, como decía antes, de jueces y fiscales, que todo el día están trabajando con esto y lo conocen perfectamente, y pueden establecer cauces de comunicación efectiva y real, con traslado real de los casos, cómo se articulan y resuelven. Podría ser muy útil. Evidentemente, hay que definir a un ciberactivista y a un ciberdelincuente; la diferencia está básicamente en para qué se hacen las cosas. A mí la curiosidad en Internet me lleva a hacer cosas que me podrían convertir en un ciberdelincuente; el cambiar un número de una URL, si me permite entrar en el buzón de otro compañero, ¿quiero delinquir?, ¿quiero entrar? No, es la mera curiosidad. El problema está ahí, en ser consciente en relación con determinadas cuestiones.

En cuanto a los ayuntamientos, ayer un compañero, con motivo de una licitación de adaptación de un ayuntamiento al Reglamento General de Protección de Datos, publicaba la noticia en Twitter. Resulta que salía la licitación justo debajo de otra. La licitación era adaptación al Reglamento General de Protección de Datos, DPD y un montón de cosas que tienen que ver con la protección de datos, y se licitaba en 14 900 euros. Al lado de esa licitación había otra licitación para comprar 500 000 bolsas para la recogida de cacas de perros valorada en 13 000 euros. Ese es el nivel de concienciación que hay sobre la importancia de estos temas en las administraciones locales. Es evidente que por mucho problema que supongan las cacas de perros, adoptar estas medidas supone un trabajo, una implicación y una responsabilidad y las administraciones más pequeñas no pueden hacerlo porque no están preparadas ni hay gente con conocimientos. Aquí hay un trabajo de coordinación de diputaciones y de comunidades autónomas, de asumir un cierto liderazgo, igual que ha pasado con los sistemas de contratación pública, por ejemplo lo de los perfiles del contratante, que acaban siendo gestionados por la comunidad autónoma en vez de por cada ayuntamiento porque no hay capacidad técnica. Hay un ámbito para trabajar en coordinación supramunicipal y poder aportar recursos para resolver esto.

Por lo que se refiere a la Directiva de derechos de autor —aquí entramos en otras cuestiones—, decía antes que hay un derecho a no ser sometido a decisiones basadas en algoritmos. Está recogido en la Ley de Protección de Datos y en el reglamento. No sé cómo se va a cohonestar lo que propone la directiva con la Directiva de servicios de la sociedad de la información, que impide la vigilancia previa de los contenidos que circulan por la red. Es decir, dentro de los mecanismos de exclusión de responsabilidad de los prestadores de servicios hay una no obligación general de supervisión. Estamos metiendo elementos de supervisión. Y más allá del conflicto normativo, no tenemos inteligencia artificial que detecte el matiz entre una parodia y una obra, por ejemplo, lo que puede provocar efectos muy importantes en la libertad de

cve: DSCG-12-CM-102

expresión, en la libertad de información en relación con los conflictos con la propiedad intelectual. Además, hay que tener en cuenta una cosa. La propiedad intelectual es el mecanismo más fácil que tenemos los abogados cuando queremos retirar un contenido de Internet. Todas las empresas de Internet cuando denuncian una infracción de derechos, aunque realmente lo que te moleste es un tema de derecho al honor o a la propia imagen, en cuanto la articulas por propiedad intelectual el prestador de servicios actúa rápidamente. ¿Esto qué quiere decir? Que se ha utilizado, se usa y se abusa de la propiedad intelectual como un mecanismo para coartar otros derechos y otras libertades, fundamentalmente la libertad de expresión y la libertad de información. Por eso es posible que en este sentido la directiva no vaya por el buen camino, aparte de que preocupa otra cosa. La necesidad de contar con mecanismos de control va a impedir que pequeñas empresas con proyectos novedosos puedan disponer de esos mecanismos y por tanto no puedan competir con Google, con Facebook y con otras grandes empresas que los van a poder implementar porque van a poder hacer la inversión necesaria para no asumir el riesgo legal y, en caso de que exista ese riesgo, poder afrontarlo. Es, pues, un mecanismo de freno a la competitividad entre empresas. Igual que el gran error de la Directiva de 1995, de protección de datos, fue que las empresas de aquí tenían que cumplir con esa ley y las empresas de Estados Unidos no. Esa es una de las razones fundamentales por las que la mayoría de las empresas de redes sociales son de Estados Unidos; no solo el ecosistema innovador, no solo eso, sino también la normativa. Ahora estamos provocando más trabas, más problemas para las empresas de aquí, porque las de allí al final lo resolverán o encontrarán formas de hacerlo.

Con respecto al anonimato, la Constitución, aunque no de manera expresa, ligándolo a lo que decía el señor Luena, reconoce un derecho al cifrado de las comunicaciones, a poder navegar por Internet de manera anónima y segura. Otra cosa es cómo lo articulemos porque realmente es complejo. Evidentemente, lo que no se debe tolerar es que alguien cometa un delito, que alguien acose, que alguien genere un problema en la red a alguien y eso no tenga consecuencias. Yo abogo por el reconocimiento de un derecho al anonimato, pero reconozco el problema que tenemos, como decía antes, a la hora de cohonestar eso con que no haya una impunidad. Desde luego, un Estado en el que se protege o se auspicia la impunidad es un Estado de derecho fallido y eso yo tampoco lo quiero. Conociendo la complicación, lo que planteaba la portavoz del Grupo Parlamentario Popular, es cierto que este debate está y va a estar ahí y de momento tiene una muy complicada resolución. La verdad es que cada vez más vamos más a sistemas automatizados, a ceder la libertad. Esa es la sensación, la percepción que tengo.

Para terminar, enlazando con la filosofía que considero que hay que seguir a la hora de regular estas novedades y estos enfoques, les recomendaría un libro que para mí fue esencial. Es del año 1997, es decir, ya tiene veinte años, *El código y otras leyes del ciberespacio,* de Lawrence Lessig. Es un ensayo magnífico entre la pulsión que ustedes tienen que tener contra quienes hacen el código informático. Ustedes son el legislador de la costa este —así los llama porque Washington está en la costa este de Estados Unidos— frente al legislador de la costa oeste, que es el que hace el código. Lo que yo pueda hacer en Internet va a venir determinado por lo que alguien programe. Él anticipaba en el año 1997 ese conflicto y lo evidenciaba de una manera tan cruda que nos ponía frente a la necesidad de resolver esa cuestión: quién va a regular lo que pasa en Internet, que al final acaba teniendo un traslado en la sociedad real. Como reflexión, para no extenderme más, creo que en ese libro se encuentra la filosofía que yo defiendo. Sobre todo la inteligencia.

Por último, los informáticos me han demostrado en mi vida que son más listos que los abogados. Cada vez que los abogados o que la legislación ponen un problema, el informático se lo salta. Esto nos obliga a tener la mente muy abierta, a escuchar, a estar pendientes y a no pensar que porque pongamos en una ley que algo no se puede hacer no se va a hacer. El que hace el código informático va a configurar el espacio de una determinada manera y lo va a poder hacer. Lo que tenemos que hacer es mantener un equilibrio, pero no pensar que poner algo en un papel va a servir de algo. Esta es la filosofía con la que debemos enfrentar estas cuestiones y afrontarlas.

Lamentando la extensión, muchas gracias por su atención.

El señor **PRESIDENTE:** Muchísimas gracias, señor Maeztu Lacalle, por su intervención y por su contestación a los distintos grupos. Sinceramente, ha sido muy interesante. Quizá hay algunas cuestiones pendientes que si las puede remitir por escrito, como comentaba el señor Luena, a la Comisión —la reforma del Código Penal o cualquier otra consideración— sería de muchísima utilidad.

cve: DSCG-12-CM-102

Muchísimas gracias y damos paso al segundo compareciente, que está en el fondo, para continuar con la Comisión. Muchas gracias.

— DEL SEÑOR LEÓN DE MORA (DIRECTOR DE LA CÁTEDRA TELEFÓNICA INTELIGENCIA EN LA RED Y DIRECTOR DEL GRUPO DE INVESTIGACIÓN TECNOLOGÍA ELECTRÓNICA E INFORMÁTICA INDUSTRIAL, TIC-150, DE LA UNIVERSIDAD DE SEVILLA), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. POR ACUERDO DE LA COMISIÓN MIXTA DE SEGURIDAD NACIONAL. (Número de expediente del Congreso de los Diputados 219/001289 y número de expediente del Senado 713/000992).

El señor **VICEPRESIDENTE:** Comenzamos dándole la bienvenida a nuestro segundo compareciente, don Carlos León de Mora, director de la Cátedra Telefónica Inteligencia en la Red y director del Grupo de Investigación Tecnología Electrónica e Informática Industrial de la Universidad de Sevilla, para informar sobre diferentes cuestiones relativas a la ciberseguridad en España. Le doy la bienvenida. Como sabe, el formato consiste en una primera intervención del compareciente —además, tiene preparada una presentación— y a continuación cada uno de los grupos en turnos de cinco minutos, de menor a mayor, formularán cuestiones y preguntas. La última intervención será para contestar lo que estime conveniente. Reiterando nuestro agradecimiento por su colaboración con esta Comisión, le doy la palabra.

El señor **LEÓN DE MORA** (Director de la Cátedra Telefónica Inteligencia en la Red y director del Grupo de Investigación Tecnología Electrónica e Informática Industrial, TIC-150, de la Universidad de Sevilla): Muchas gracias, señor presidente, y muchas gracias por la oportunidad que se me brinda de comparecer ante esta Comisión para trasladarles algunas reflexiones del ámbito que están tratando. He traído una presentación. Una de las últimas veces que he tenido que hacer una exposición me preguntaban: ¿usted venía a contar algo o a traer un *power point?* Yo traigo un *power point* para apoyarme, pero espero que les pueda contar algo de interés.

He estado siguiendo las comparecencias que han tenido lugar en esta Comisión —prácticamente todas— y el primer reto que me planteé fue qué podía yo aportarles. Hay temas que han salido reiteradamente y que han ido apareciendo en una comparecencia tras otra. Se ha hablado de formación, de investigación y desarrollo, de los aspectos económicos, de la seguridad nacional, etcétera. Al final, después de pensarlo un poco, quiero orientar la presentación hacia dos ámbitos en los que puedo aportarles alguna experiencia. Yo soy un académico. Soy catedrático de la Universidad de Sevilla y, por tanto, mi especialidad es la investigación y la formación, y en ese ámbito es en el que voy a enfocar mi comparecencia.

Si me lo permiten, vamos a empezar por una pequeña broma. **(Muestra una imagen con una casete y un bolígrafo).** Esta es una transparencia que les suelo poner a mis alumnos de postgrado cuando imparto clases de doctorado o de master. Como se imaginan, son chicos y chicas de poco más de veinte años y sorprendentemente no ven la relación que existe entre los dos objetos. Por la edad media de las personas que están aquí presentes entiendo que todos la conocen, pero me sirve para ilustrarles sobre que el desarrollo de la tecnología ha ocasionado un desarrollo exponencial de la sociedad. Remontándonos a los primeros tipos de sociedad, la sociedad agraria duró miles de años; la industrial, centenares; la de Internet, décadas, y estamos entrando en la sociedad de los datos, en la sociedad de la inteligencia artificial, con lo cual crece la velocidad de aceleración y no sabemos exactamente hacia dónde vamos. Ese impulso viene dado por la evolución de la tecnología. La tecnología se expande cada vez más rápido. Si desde la introducción del teléfono hasta llegar a los cien millones de usuarios pasaron setenta y cinco años, las últimas aplicaciones en redes sociales que todos seguramente llevamos en nuestro teléfono han tardado pocos años e incluso meses en el caso de las más recientes. Eso nos representa retos desde los dos puntos de vista que les pensaba comentar. También para los que dedicamos nuestra labor a la formación comporta un reto importante, porque vivimos etapas de aceleración y muchas veces no tenemos las herramientas ni los instrumentos que nos permitan responder adecuadamente a las necesidades que la propia sociedad nos va marcando.

El mundo de la ciberseguridad que, como les digo, se enmarca dentro de un mundo tecnológico acelerado y complejo es difícil de abarcar desde el punto de vista del ser humano. Estaba escuchando la comparecencia anterior y se ha hablaba de aspectos legales y de controlar los algoritmos, pero cada año se producen más de 111 billones de líneas de código, billones europeos. Como comprenderán, auditar todo esto resulta ciertamente complejo. Internet llegará a 6000 millones de usuarios dentro de pocos años.

cve: DSCG-12-CM-102

Cada vez habrá más coches conectados —hablaremos del coche autónomo después— y el volumen de datos que almacenamos como contenido digital alcanzará en 2020 cincuenta veces los que tenemos hoy en día, una cantidad del orden de 96 petabytes, siendo un petabyte un billón de terabytes. Como ustedes comprenderán, todo esto es complicado de manejar. La aceleración de la tecnología se traslada a una aceleración social. La vida media de las empresas se reduce y probablemente dentro de diez o quince años el 30 % de las empresas que existen hoy en día habrán desaparecido. Creo que ha comentado algún compareciente anterior que la diferencia entre el mundo físico y el mundo digital se difumina —por ejemplo, la mayor empresa de distribución del mundo no tiene una sola tienda— y el centro de la economía se está desplazando hacia la economía basada en los datos. Si miramos las cinco mayores empresas por capitalización bursátil —es decir, las cinco mayores empresas del mundo—, son cinco empresas tecnológicas con una vida relativamente corta y para encontrar la primera empresa industrial con cierta trayectoria no tenemos que ir al séptimo puesto de la lista. Además, curiosamente ninguna de las cinco mayores empresas es europea. Para complicar más la cuestión, tenemos algo que sigilosamente ha llegado a nuestras vidas pero que no tenemos conciencia del impacto que va a tener a corto plazo, que es la inteligencia artificial: máquinas que son capaces de actuar en determinados aspectos muy concretos de una forma similar a como lo hacemos los seres humanos. Es una tecnología relativamente «autónoma» —y permítanme que use la palabra autónoma entre comillas—. Esto nos parece muy exótico, pero pensemos que en el mercado continuo el 50 % de las operaciones de trading en las bolsas del mundo se hacen por bots de inteligencia artificial o que los coches autónomos ya están circulando y que en breve —cuando lo autorice el legislador— estarán en carreteras. Es una tecnología que está aquí y que va a ser ubicua. Dentro de pocos meses empezarán ustedes a ver —me lo recordaba el compareciente anterior— altavoces inteligentes en nuestro domicilios y que responderán a órdenes de voz con inteligencia artificial, la misma inteligencia que tenemos ya en los teléfonos móviles; claro que estos altavoces, aparte de recibir órdenes, escucharán todo lo que hacemos. Esa es otra cosa.

¿Cómo impacta esta tecnología y esta aceleración en el ámbito de la ciberseguridad y cómo podemos enfrentar las necesidades de formación que evidentemente tenemos? Creo que también se ha hecho referencia en comparecencias anteriores a los informes globales de riesgo del Foro Económico Mundial, que marcan la ciberseguridad como uno de los factores clave, esenciales y más críticos en cuanto a riesgo de conflicto y de inestabilidad en los próximos años. Los riesgos en ciberseguridad están creciendo y es curioso porque las inversiones son mayores que nunca. También están creciendo mucho las inversiones en ciberseguridad, luego hay que plantearse que algo debemos de estar haciendo mal. Si los riesgos crecen y cada vez invertimos más, esta va a ser una carrera que no sabemos si va a ser sostenible. Además, un informe geoestratégico indica que las infraestructuras críticas van a ser objeto de ataques de ciberseguridad y, en algunos casos, esos ataques van a estar respaldados por Estados. Por tanto, la ciberseguridad es de los riesgos más impactantes y también más probables. Les voy a dar algunos datos que ya se han comentado aquí, pero que son interesantes. El número de ciberataques por empresa se duplica prácticamente cada año. Se estima, por ejemplo, que el año pasado en Estados Unidos se pagaron más de un billón de euros por infecciones de *ransomware* a la gente que infecta los ordenadores y pide un rescate. En la red oculta —que, aunque no es accesible por los buscadores que normalmente utilizamos, tiene cincuenta veces el tamaño de la red a la que accedemos— se vendieron durante el año pasado más de 500 millones de dólares en *malware, software* especializado en buscar debilidades y realizar ataques de ciberseguridad. Tenemos dispositivos de Internet de las cosas que van a ser ubicuos. Y un dato que a mí me llamó la atención es que la Agencia Europea de Aviación reporta que hay más de mil ataques de ciberseguridad a sistemas de navegación aérea al mes. Afortunadamente por ahora parece que ninguno de estos ataques ha ocasionado ningún conflicto grave, pero el riesgo potencial está ahí. El cibercrimen moverá en los próximos cinco años 8 trillones de dólares americanos. Eso conlleva un riesgo. En aras de la defensa, podemos tratar de fragmentar Internet —esto ya lo están haciendo algunos Estados—, podemos poner puertas, de forma que Internet no tenga una conectividad global. Si además tenemos un riesgo de ataques, esa fragmentación se puede ver exacerbada. También está todo el tema de ciberarmas y ciberconflictos, así como el de los *password,* esos que todos tenemos y que no sabemos cómo recordar. A nivel mundial, habrá que proteger trescientos billones de *password* en el año 2020.

En dimensión humana, este es un riesgo verdaderamente complejo de manejar, porque, además, los atacantes evolucionan, aprenden, se sofistican, los ataques son cada vez más complejos, más difíciles de detectar. En la mayoría de los casos lo que se busca es un beneficio económico, según los últimos análisis, pero también aparecen interferencias de otros actores del ámbito geoestratégico que pueden

cve: DSCG-12-CM-102

buscar otros usos maliciosos de la ciberseguridad. Entre los cinco sectores más atacados están la salud, los procesos de fabricación, las finanzas, lo cual no nos llama mucho la atención, pero también los sectores gubernamentales, que es uno de los focos principales de los ataques, que además está creciendo en los últimos años. La mayoría de atacantes siguen siendo cibercriminales, pero en los datos ya aparece reflejada la presencia de actividades por parte de Estados extranjeros, *hacking* ético y demás, pero que no generan en principio una dificultad económica.

¿Cómo enfrentamos la tarea de la formación en este escenario? La Estrategia de Ciberseguridad Nacional ya menciona explícitamente la necesidad de formar talento, en este caso en nuestro país, en los ámbitos que tienen que ver con la ciberseguridad, así como fomentar también la investigación y desarrollo en ese ámbito, incluso se menciona la cooperación con las universidades. Es un océano complejo de navegar porque, además, es muy cambiante. Por tanto, tenemos que tratar de buscar herramientas. El Comité Europeo de Normalización clasifica los perfiles, dentro del ámbito de las tecnologías de información, en una serie de familias, que describen, básicamente, qué tipo de trabajo se realiza en ese ámbito. Si buscamos lo que tiene que ver con la ciberseguridad, hay dos perfiles que aparecen, que son el gestor de seguridad y el especialista en seguridad, básicamente enfocados ahí. Esos perfiles, a su vez, se desarrollan en competencias, en E-competencias, que indican qué tareas hay que conocer y hay que manejar para desarrollar un determinado trabajo. Pues bien, basándonos en esos perfiles, se puede elaborar un catálogo de formación, de titulaciones, que nos puede ayudar a las universidades y a otros entes de formación a planificar qué formación es necesaria en el ámbito de la ciberseguridad a corto y a medio plazo, así como a establecer un sistema de acreditación de esa formación, porque tan importante es hoy en día que la persona reciba una formación como que sea capaz de acreditarla frente a terceros. Lo que dicen las estadísticas y lo que me trasladan las empresas —conozco bastante bien el sector de la I+D— y los organismos es que realmente es difícil en nuestro país encontrar talento formado en ciberseguridad. Normalmente, se busca a gente que tenga certificaciones profesionales —de esto hablaremos un poquito más adelante— con experiencia práctica. En fin, esto casi es un mirlo blanco, si me permiten la expresión. Además, nos hacen falta puestos técnicos. Yo soy tecnólogo y la tecnología me parece muy bonita y muy interesante, pero tiene una parte árida y dura. Lo que hace falta son perfiles técnicos, gente que se arremangue y sea capaz de enfrentarse a estos retos. Curiosamente, hay mucha menos falta de talento en el ámbito de los perfiles de gestión, de los perfiles de jefatura de este tipo de asuntos. Tenemos un problema adicional, que es un problema crónico en el ámbito tecnológico, no solo en nuestro país sino a nivel del mundo occidental, que es el tema de la brecha de género. Tenemos muy poco talento femenino en el ámbito de las ingenierías y, en particular, en el ámbito de la ciberseguridad la situación es todavía peor. Sin embargo, es algo atractivo, porque todos los informes y toda la realidad marcan que hay un incremento de salarios. Es un sector que está muy bien remunerado. Esto tiene que ser una palanca que podamos trasladar a nuestros estudiantes, de manera que se formen en este tipo de ámbito. Y como no hay talento y el talento es muy caro, cuando pasa eso llega la tecnología y se avanza hacia la automatización de los procesos. Si automatizamos un proceso, disminuimos la necesidad de contratar a una determinada fuerza de trabajo, y eso lleva a lo que vamos a comentar después, a la utilización de la inteligencia artificial en este ámbito. Hay un montón de puestos de trabajo a cubrir y se prevé un gasto de formación enorme; se estima que el gasto en formación superará los 10 billones de dólares en el año 2027. Este es un mercado que también hay que atender, porque la mayoría de solicitantes que optan a un puesto de trabajo no tienen la formación adecuada —esto nos dicen las empresas que se dedican a ciberseguridad— y, en muchos casos, hay que formarles. Eso se suma al problema crónico que tenemos en toda la Unión Europea de carencia de competencias digitales de la población en general. España está en una zona media, no está ni mejor ni peor que en otros países, pero sí que hay que inculcar estas habilidades, y eso ya no es tanto cosa de la educación universitaria, que también, sino que en todas las etapas del desarrollo formativo de las personas hay que ir inculcando estas habilidades digitales, porque, si no, no tendrán ninguna posibilidad de insertarse en el futuro en el mercado de trabajo.

¿Cómo está la situación en España? ¿Cómo estamos nosotros? ¿Dónde acude alguien que quiera hacer algo de ciberseguridad? ¿Dónde puede formarse? Les confieso que a mí me sorprendieron los datos. En España, actualmente, se imparten cuarenta y ocho másteres en aspectos relacionados con la ciberseguridad. Es verdad que bajo la palabra máster se esconden muchas cosas **(risas),** sin entrar en más consideraciones, pero veinticinco son *online,* cosa normal en un perfil de este tipo; muchos están amparados por grandes empresas —algunas personas de estas corporaciones han estado compareciendo

cve: DSCG-12-CM-102

aquí— que apoyan, realizan prácticas y orientan un poco a la formación; quince son impartidos en universidades públicas —para el número de universidades públicas no es una cifra demasiado importante—; únicamente cuatro son títulos oficiales, es decir, son títulos que están certificados por el Ministerio de Educación, y el resto son de formación heterogénea. Por eso digo que dentro de la palabra máster, desde el punto de vista de la formación, se puede esconder desde un máster oficial perfectamente tasado y organizado hasta títulos creados de una forma más rápida pero también más heterogénea; y algunos asocian certificaciones profesionales. En realidad, existen ochenta y tres instituciones, al menos que yo haya podido encontrar, que imparten formación en ciberseguridad en España, y de ellas solo veintisiete son universidades, el resto son escuelas de negocios, empresas que tienen sus cursos, etcétera. En la última reunión de hace una o dos semanas de la conferencia de decanos y directores de todas las escuelas de ingeniería informática y de informática de España, aparecía que el perfil de ciberseguridad es uno de los que tienen una demanda importante por parte de los empleadores, pero que no cubrimos porque no somos capaces de formar ese talento. Es verdad que no generamos el suficiente talento ni el suficiente número de egresados en un montón de áreas que tienen demanda laboral. Hacemos lo que podemos, pero es que no recibimos más solicitantes. Por otra parte, en un ámbito tan concreto como este se buscan certificaciones profesionales ante la variabilidad que hay de la formación y, al ser un aspecto tan nuevo, se buscan certificaciones profesionales, la mayoría internacionales, que certifiquen que las personas que realizan estas tareas tiene unos conocimientos.

La Estrategia de Ciberseguridad Nacional habla también de la necesidad de invertir en investigación y desarrollo, en desarrollar un tejido de I+D en ciberseguridad. Esto ha salido también en comparecencias anteriores. De hecho, las grandes empresas, Telefónica o grandes consultoras, tienen sus propios departamentos de ciberseguridad y hacen I+D en ciberseguridad. Instituciones, como Incibe y CERT, también colaboran con universidades en este ámbito, pero es verdad que en los últimos dos o tres años han surgido iniciativas de I+D muy dispersas por el territorio, están por casi todo el Estado. Aquí el riesgo que tenemos es el de los recursos, como en todo. Tenemos que plantearnos como país si este es un aspecto crítico. Si lo es, en la investigación podemos hacer milagros, pero sin una inversión es difícil. El presupuesto medio de estos centros oscila entre los 3, 4 o 5 millones de euros, en el mejor de los casos, anualmente. Tenemos que ver en qué liga queremos jugar y cómo queremos posicionarnos en ese ámbito.

Paso rápidamente al otro aspecto que les quería comentar, el ámbito de la inteligencia artificial, que suena a algo exótico pero que es algo que ya está aquí, que está siendo explosivo y va a seguir siéndolo en los próximos años, básicamente porque disponemos de una cantidad enorme de datos, algo que no habíamos tenido hasta hace una década. Big Data, redes sociales, Internet… El hecho de que todas las transacciones estén digitalizadas ponen a disposición de los sistemas de aprendizaje automático una cantidad ingente de datos. La potencia de cálculo o la potencia de cómputo también ha subido en rendimiento y ha bajado de coste; cada vez tenemos gente más formada a nivel mundial en estas tecnologías que antes suponían algo un poco exótico y los algoritmos también se han perfeccionado. Eso hace que, según todas las consultoras, la inteligencia artificial vaya a ser la tecnología estratégica del siglo XXI; de hecho, ya lo está siendo. Las inversiones que se prevén son absolutamente gigantescas. La Unión Europea prevé que durante la próxima década deberemos ser capaces de llegar a los 20 billones anuales de inversión. Las mayores empresas basadas en datos —esas que comentábamos anteriormente— invierten miles de millones, en este caso de dólares, en investigación en inteligencia artificial y esta tecnología va a afectar a todas las áreas, tanto a las de gestión como a las áreas económicas.

Hay un aspecto sobre el que también tendremos que reflexionar, ya que esta cuestión va a transformar la forma en que se trabaja y va a destruir puestos de trabajo. Es verdad que creará otros, pero va a destruir empleo de una forma más rápida que lo que ha pasado en revoluciones anteriores. Tendremos que ser capaces de adelantarnos a eso y ver cómo conseguir que dicha destrucción sea compensada por la creación de nuevos puestos de trabajo, porque, en mi opinión, la destrucción va a venir inexorablemente acompañada por la creación en otros ámbitos.

La inteligencia artificial afecta a un montón de tecnologías, no me voy a entretener en ello, y en cuanto a las aplicaciones —la transparencia simplemente pretendía demostrar que están en todas partes—, yo he querido resaltar, debido al ámbito de la comparecencia, que ya se está aplicando en el gobierno de los ciudadanos. A lo mejor en este país se concentra en un foco muy concreto, pero en otros ya se está haciendo, y hay decisiones que ya se están tomando sobre la base de algoritmos de inteligencia artificial. Algoritmos, por cierto, que para mí, que he dedicado a esto tiempo, son cajas negras. Es decir, no está

cve: DSCG-12-CM-102

muy claro por qué toman la decisión que toman y que también pueden tener sesgos, porque el programador cuando los programa y los datos con los que se entrenan pueden tener sesgos, y ese sesgo se puede trasladar al algoritmo y, por tanto, a las decisiones que ese algoritmo toma. Es muy cómodo porque permite tomar muchas decisiones de una forma muy rápida.

Les hablaba del aspecto estratégico de esta tecnología. La inteligencia artificial es un aspecto geoestratégico, y tan estratégico es que las principales potencias del mundo están reflexionando sobre el tema. La Presidencia de los Estados Unidos de América ya elaboró en los años 2016 y 2017 dos informes sobre cuál debe ser el futuro y el posicionamiento del país en el ámbito de la inteligencia artificial. La estrategia industrial del Reino Unido marca, entre los cuatro retos que tiene el Reino Unido para los próximos años, como primero la inteligencia artificial, y el reciente informe Villani, a instancias del primer ministro francés, también reflexiona sobre esto y señala una cosa que me llamó la atención, y es que o Europa se posiciona adecuadamente en esta cuestión o podemos convertirnos en lo que denomina como cibercolonia. La Unión Europea, a través de la Comisión Europea, ha instado a la elaboración de una estrategia de inteligencia artificial para Europa que debe estar preparada a finales de este año. Otras potencias, como Rusia, China, Israel y Canadá, tienen sus propios planes estratégicos, y nosotros en España tenemos uno en fase de elaboración, lo cual es una gran noticia. Hace pocos meses empezó a trabajar una comisión con nueve expertos, a instancias de la anterior Secretaría de Estado para la Sociedad de la Información, y en próximos meses tendremos las conclusiones.

Realmente, casi todos esos informes —ahora veremos cómo enlaza esto con la ciberseguridad— inciden casi en las mismas cosas. Estamos haciendo la transición hacia una economía basada en datos y es clave evitar el control de los mismos. Si esos datos están en poder de equis corporaciones, que muchas veces tienen más datos de los ciudadanos que los propios Gobiernos, y ni los Gobiernos ni los ciudadanos ni otras empresas pueden a acceder a esos datos, pueden surgir enormes riesgos. Es preciso, como insisten todos, potenciar la investigación, la creación de centros interdisciplinares, fomentar la formación y los temas que comentaba anteriormente de impacto futuro en el mercado laboral para ver cómo podemos mitigar o solucionar dicho impacto, y como es clave para la transición hacia una economía verde. Cada vez se trabaja más en estos informes —también se está haciendo por otra parte—, y ahí creo que hay un recorrido interesante en cuanto a entender los aspectos éticos y los aspectos legales del uso de estos algoritmos, que, como les decía, son cajas negras, pueden tener sesgos e impactar en la privacidad de forma grave, puesto que una cosa es disponer de datos y otra tener la capacidad de extraer información de los mismos, y los sistemas de inteligencia artificial permiten hacer eso con mucha cantidad de datos. Por otra parte, enlazando con la ciberseguridad, quiero referirme a la seguridad y a la protección de los propios sistemas de inteligencia artificial o el uso de los sistemas de inteligencia artificial como vector de defensa o de ataque en el ámbito de la ciberseguridad; ciberseguridad que también se menciona en estos informes estratégicos que les comentaba antes como un aspecto absolutamente clave dentro del despliegue de la inteligencia artificial. No es que esto venga, es que ya está aquí. Desafortunadamente, no tengo datos de la Unión Europea, pero el 80 % de las empresas que se dedican a ciberseguridad en USA utilizan inteligencia artificial —cerca del 70 % de las que lo hacen en Japón— y las inversiones son gigantescas también, como se puede ver en la transparencia.

¿Dónde se va a utilizar la inteligencia artificial? Se va a utilizar para defenderse, pero también para atacar. Como cada vez tenemos más datos y los sistemas de decisión van a ser más complejos y comportan más variables, aumenta lo que en ciberseguridad se conoce como la superficie de ataque. Y como la superficie de ataque aumenta, no tenemos personal y el problema es más complejo, aquí llega la inteligencia artificial para echarnos una mano y crear ciberescudos. Pero, claro, cuando se crea el ciberescudo, el atacante también crea otra ciberarma basada en inteligencia artificial para tratar de romperlo, y entonces entramos en el círculo que tenemos aquí. En este sentido, corremos el riesgo de que los sistemas sean tan autónomos que se ataquen y se defiendan de ellos mismos. Si tenemos ocasión, después les contaré alguna anécdota al respecto.

Respecto a dónde se va a integrar la inteligencia artificial en ese sentido, la ciberseguridad siempre aparece como uno de esos aspectos clave. ¿Dónde se va a utilizar? Como decía, se está utilizando ya en la prevención y detección de ataques, pero también se va a tener que utilizar en la securización de los dispositivos de Internet de las cosas, que van a explosionar de forma tremenda. Todos están conectados a Internet, todos recogen datos y todos transmiten datos, y con esos datos se pueden conocer muchas cosas, se puede sacar mucho rendimiento a los mismos.

cve: DSCG-12-CM-102

Se están utilizando algoritmos ya en el ámbito del análisis de los *social media,* de las redes sociales, para determinar *fake news,* comportamientos potencialmente anómalos, difusión de información terrorista, etcétera, gracias a la capacidad que tienen de analizar automáticamente mucha cantidad de información. Se están también empezando a integrar en tecnologías como *blockchain* para blindar las transacciones financieras y siempre, afortunadamente, en una aproximación híbrida. Por ahora no son sistemas absolutamente autónomos, sino que siempre han de colaborar o trabajar en paralelo con los seres humanos, pero esa introducción va a llevarnos a un riesgo, y es que en principio el sistema de inteligencia artificial no tiene una voluntad propia; tiene la voluntad que se le programe, pero cualquier combinación de capacidades y de voluntad es programable. Podríamos tener mucha capacidad con mucha maldad, o lo contrario, o podríamos tener sistemas perfectamente diseñados pero que se hackeen y entonces empiecen a operar de una forma diferente a como está previsto que lo hagan.

Los sistemas de inteligencia artificial ya están combatiendo fraudes concretos, y los atacantes también. Por ejemplo, en el ataque *Ransomware* tan famoso que tuvimos hace relativamente poco, los algoritmos de ataque de inteligencia artificial ya no encriptan todos los datos de un disco duro, sino que buscan qué datos son los más sensibles en cada disco duro que encriptan, con lo cual, sube el valor de la transacción. O el clásico correo que supongo que todos habrán recibido de alguna persona conocida que de una forma relativamente burda suplanta la identidad y trata de que uno pinche en un *click,* detrás del cual está el malo esperando para hacernos algo; los sistemas de inteligencia artificial se meten dentro de nuestros ordenadores y se ponen a observar qué estilo de escritura tenemos, con quién hablamos, cuántos párrafos escribimos, con lo cual, la capacidad de suplantación que tienen es muchísimo más grande. De hecho, se trata de un tema al que hay que tener cierto respeto, porque asusta. En todo este ámbito, si me permiten insistir sobre ello, existe el riesgo de monopolio real de los datos, que están relativamente en pocas manos y no precisamente cerca de las nuestras.

Por ir terminando, simplemente voy a insistir —igual que insistía en la necesidad de hacer I+D+i— en ciberseguridad en especial. Ya lo está viendo la Comisión Europea porque en el nuevo programa marco, en los documentos preliminares, se introduce la inteligencia artificial para ciberseguridad como una de las líneas estratégicas esenciales y comienzan a atisbarse a nivel europeo los primeros centros de investigación de excelencia en inteligencia artificial y en ciberseguridad. Esto es algo que tendremos que reflexionar, si a nivel de país tenemos que colocarnos en esta carrera.

Podría contar muchas más cosas, pero en aras de la brevedad, aquí lo dejo.

El señor **VICEPRESIDENTE:** Muchísimas gracias, señor León de Mora, por su intervención y por sus aportaciones. Han quedado algunas cosas pendientes pero va a tener una segunda intervención para poder incorporar lo que estime conveniente y oportuno.

Pasamos ahora a dar la palabra a los distintos grupos, como siempre, de menor a mayor. Señor Legarda, por el Grupo Vasco.

El señor **LEGARDA URIARTE:** Muchas gracias, presidente.

Simplemente quiero agradecer al ponente su exposición, que ha sido tan densa que en este momento no tengo ninguna pregunta. Tendría que reflexionar sobre todo lo oído.

El señor **VICEPRESIDENTE:** Señor Salvador, por el Grupo Ciudadanos.

El señor **SALVADOR GARCÍA:** Muchas gracias, señor presidente.

En primer lugar, quiero felicitarle por su intervención. Usted ha dicho que ha visto muchas de las intervenciones que se habían realizado anteriormente y que quería encontrar el hueco en el mercado para trasladarnos cuestiones que no se hubieran visto. He de decir que lo ha conseguido sobradamente. Después de tantas comparecencias —todas ellas interesantes, independientemente de que algunas hayan redundado en algunos datos—, puedo decir que su aportación ha sido fantástica y que podría haber hecho dos comparecencias más porque ha aportado información permanentemente, producto de la investigación que usted mismo está desarrollando. Nos ha sintetizado un trabajo de mucho tiempo, un análisis no solamente de cómo han evolucionado las cosas sino sobre todo de cómo pueden evolucionar.

Estamos en un mundo marcado por la inteligencia artificial, por el Big Data, el Internet de las cosas, con profundos cambios que va a haber en el mercado laboral, y me ha gustado mucho que se detuviera en eso porque o reflexionamos desde esta casa y desde otros ámbitos y empezamos a pensar en el mercado laboral del futuro o empezaremos a encontrarnos noticias de ERE en los periódicos y problemas

cve: DSCG-12-CM-102

sociales en la calle y llegaremos tarde a intentar solucionarlos. Esa aportación de soslayo en este momento nos tiene que hacer tener muy en cuenta que debemos actuar con tiempo sobre todas estas cuestiones. Usted se ha detenido bastante a la hora de describir cosas alrededor de la inteligencia artificial. Evidentemente, la inteligencia artificial es programada, alguien la ha programado y alguien la ha desarrollado, y esos algoritmos salieron de algún sitio, pero luego se retroalimenta bastante sola. Al final, el factor humano va a ser necesario pero bastante menos. Esto me recordaba lo que usted decía de ataque-defensa-ataque-defensa. Al final, es como una partida de ajedrez jugando contra una máquina que siempre tiene una jugada y, si jugara una máquina contra otra, una de ellas terminaría ganando. El caso es que termine ganando la buena en vez de la mala. Por eso también me ha gustado el dato que ha plasmado sobre que el mantenimiento de la inteligencia artificial y esa actualización debe ser un factor muy a tener en cuenta.

Las administraciones y las instituciones contamos con algo a favor a priori y es que hay que adoptar medidas que tienen que proteger a todo un país, por tanto, la inversión de medios que se haga tiene que ser suficiente. Después está ese mantenimiento que usted decía. Los malos tendríamos que dividirlos en categorías y me preocupa cuando usted menciona aquí Estados. Me ha gustado mucho algo que no sé si ha comentado en su intervención pero que sí estaba en la transparencia, que decía que no hay convenciones para los ciberconflictos, algo que consideramos que tiene que ser absolutamente fundamental. Sabemos que detrás de determinado tipo de ataques pueden estar incluso Estados y a nivel político en la comunidad internacional eso no tiene ninguna traslación en ninguna conferencia, donde alguien acuse públicamente a un Estado de que le haya atacado, muestre pruebas y eso suponga algún tipo de condena o de compensación de un Estado a otro. Eso es algo absolutamente fundamental porque, si no, sería como una especie de videojuego que se está jugando por detrás sin obtener ningún tipo de resultado, más allá del daño que hayan conseguido provocar. Por tanto, quiero agradecerle nuevamente su intervención y todo lo que ha aportado.

En relación con el tipo de los puestos, me gustaría que describiera un poquito más esta cuestión. Ha hablado del tema de los expertos en ciberseguridad y ha dicho dónde se puede obtener parte de la formación que hay ahora, que es incompleta y que tendrá que salir de ese catálogo de necesidades para darle respuesta. Yo recuerdo una época en la que el número de informáticos que se necesitaban para cubrir las necesidades a nivel mundial era muy superior al número de los que se producían dentro de las universidades. Entonces se entró en la etapa en la que eran las empresas privadas las que formaban a sus propios informáticos. De hecho, recuerdo como anécdota que IBM quería personas con una titulación superior, y a partir de esa titulación superior o media, ellos se encargaban de darle toda la formación. Quiero preguntarle a usted, que viene también del mundo de la universidad, si piensa que al final, si no hay una oferta pública que regule y controle toda la demanda de formación de profesionales necesaria, no puede pasar un poco igual, que sean las grandes corporaciones, las grandes multinacionales, las que terminen haciendo sus propios expertos y profesionales de la ciberseguridad, lo que cubriría su necesidad, pero no estaríamos poniendo esa formación al servicio del interés general. Me gustaría que nos pudiese dar algo más de visión sobre esto.

A la hora de hablar de los profesionales ha descrito el tema de los técnicos, gestión y nivel ejecutivo. Me gustaría, si pudiera, que entrara un poco más en ello, porque yo le voy a hacer un reconocimiento. Hace unos días, a mi hija Natalia, que ha terminado Marketing e investigación de mercados y que ahora está pidiendo un máster, yo le decía: Natalia, métete en ciberseguridad. Le hablé de los datos que estamos escuchando aquí y entonces ella me dijo, como es lógico, que ahora mismo casi todo lo que se está pidiendo son personas que tengan ingenierías informáticas. Como yo no creo que las ingenierías informáticas den el número suficiente de profesionales necesarios, le pediría algún consejo tanto para mi hija como para las hijas de todos los que en un momento determinado puedan ver que la ciberseguridad es un campo de futuro y que tienen otras titulaciones que se pueden acercar pero que no están formadas de manera especializada sobre ello. Básicamente, repito, ha conseguido en una intervención breve aportarnos muchísima información, que va a ser muy útil para esta Comisión.

Muchas gracias.

El señor **VICEPRESIDENTE:** Muchas gracias, señor Salvador. Será contestado oportunamente al final sobre esa recomendación que es para su hija pero que es para todos.

Por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, el señor Comorera tiene la palabra.

cve: DSCG-12-CM-102

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

Muchas gracias al compareciente por la abrumadora información. Como ya han dicho mis predecesores en el uso de la palabra, nos hemos quedado sorprendidos por toda esta tormenta de datos que nos ha aportado, para lo que necesitaríamos, al menos en mi caso, varios días para poder procesarlos. También quiero decirle que me he quedado bastante asustado por algunos datos que nos ha dado, como el tema de los ataques en los vuelos. Era un dato que no conocía y realmente choca el estado en que puede hallarse el tema de la ciberseguridad.

Un tema en el que me gustaría que entráramos un poco es en el del control de los datos, que ha dicho usted que estaba en pocas manos. Yo creo que con el insuficiente recorrido mediático que debiera, el tema de Facebook, que creo que se encuentra en medio de una de sus mayores crisis porque ya son varias las instituciones gubernamentales y supranacionales que han pedido su comparecencia por el tema de la venta de datos de más de cincuenta millones de personas a terceros, que creo que conlleva unos riesgos y una facilidad de recortes de derechos al alcance de cualquier agente en el ciberespacio interesado en controlar y espiar a la ciudadanía. Desde el Poder Legislativo, ¿que podríamos hacer para legislar y controlar estos riesgos?

Por otro lado, me gustaría conocer su opinión sobre la cooperación entre el sector público y el sector privado en el intercambio de información y en relación a la inversión que se está haciendo en ciberseguridad. Me imagino la respuesta, me dirá que es insuficiente. Dentro de la medida de lo posible, a lo mejor estamos muy lejos en inversión en ciberseguridad con respecto a otros países, como Estados Unidos o el Reino Unido.

Desde el punto de vista de la educación y de la formación reglada, temas que también hemos defendido varias veces en esta Comisión desde nuestro grupo, me gustaría conocer su opinión acerca de cómo debería adaptarse la formación reglada a lo que realmente necesitamos.

También quisiera conocer su opinión sobre la Cátedra Telefónica Inteligencia en la Red, de la Universidad de Sevilla, que desde 2009 —si no tengo mal los datos— viene celebrando numerosas jornadas y conferencias, qué aspecto destacaría de esos nueve años de funcionamiento y qué conclusiones han derivado de concursos como el HackForGood, de qué manera nos pueden servir en la labor de detección y promoción de talento, en el marco de las nuevas tecnologías de la información.

Muchas gracias.

El señor **VICEPRESIDENTE:** Muchísimas gracias.

Por el Grupo Socialista, tiene la palabra el señor Raffo.

El señor **RAFFO CAMARILLO:** Gracias, presidente.

En primer lugar, quiero sumarme al agradecimiento al profesor Carlos León, no solo por su presencia, que también porque es un esfuerzo, sino por lo que ha significado el trabajo previo que ha tenido que realizar para facilitarnos lo que enmarca el debate y el conocimiento sobre la realidad en la que nos estamos desenvolviendo actualmente. Creo que la intervención de hoy —ha habido alguna otra que ha apuntado algo en este sentido, pero quizás esta mucho más— demuestra que la realidad supera a la ficción totalmente, superamos los argumentos de películas, entre comillas, como *RoboCop* y alguna similar, donde aparecen algunas cosas muy curiosas, o nos situamos también en novelas como *Un mundo feliz* y *1984*. Lo que pasa es que no hace falta tener una actitud de miedo ni de preocupación ante esto. Estamos en una revolución, como fue la industrial y otras posteriores, y la capacidad del ser humano para adaptarse, crear y beber de esa fuente de oportunidad, en líneas generales, no ha sido mala, al menos en lo que la mayoría de países de todo el planeta se han ido sumando progresivamente, por suerte; no tanto como habríamos deseado los que estamos aquí, que fuera en beneficio del mayor número de personas posible, pero es verdad que ha sido una oportunidad para la mejora de las condiciones de vida de las personas.

Como se ha centrado en dos aspectos fundamentales, en los que creo que ha profundizado bastante, al tiempo que ha dejado algún interrogante o reto, quiero preguntar sobre dos aspectos fundamentales. Uno tiene que ver con la formación, lógicamente. Ha estado interesante y, además, creo que ha sido exhaustivo en los puntos que ha tratado y cómo lo ha enmarcado. Me refiero a la ciberseguridad, teniendo en cuenta el papel que deben jugar los poderes públicos en lo que significa el gobierno de la realidad y de las situaciones que vive una sociedad determinada en un tiempo concreto de la historia. ¿Qué sería necesario impulsar desde los poderes públicos y, en concreto, desde el Legislativo o el Gobierno de este país para que la universidad, el campo de la FP o, en general, la educación desarrollaran iniciativas que

cve: DSCG-12-CM-102

realmente estuvieran adaptadas a esta nueva realidad, que es compleja y difícil? Creemos que con el capital humano que hoy existe —tenemos un ejemplo hoy, como en muchos de los comparecientes que han venido— se pueden desarrollar actuaciones bastante importantes para que nuestro país esté en un buen nivel de desarrollo de lo que estamos tratando.

En cuanto a las cajas negras, creo que es una buena denominación. Al final, esas cajas negras necesitarán también el papel que deben desempeñar los propios poderes públicos, como en la cuestión anterior. Tendremos que hacer algo en la regulación. ¿Qué nos recomendaría en cuanto a iniciativas que impulsaran que los poderes públicos tuvieran en cuenta este concepto que nos acaba de trasladar? Es verdad que hoy en día hay empresas, fundamentalmente del sector privado, que manejan gran cantidad de información, que, una vez que la trabajan, la trasladan a otros elementos para tomar decisiones, y, vinculada a la inteligencia artificial, puede significar que el papel del poder público, si no ejerce, quede totalmente superado por intereses particulares e individuales, que en la historia siempre han sido egoístas. Me refiero al papel del poder público a la hora de regular esa situación que tiene que ver con estas cajas negras, entre comillas, fruto de la incorporación de la inteligencia artificial.

Finalmente, ha planteado otro aspecto interesante, que es la elaboración de un libro blanco por una comisión técnica de expertos. Dirigiéndome a la propia Comisión y a la Mesa, quizás podríamos contar con la posibilidad de la comparecencia del coordinador o responsable de la elaboración de este libro blanco, quizás pudiéramos encontrar un hueco entre las comparecencias que ya tenemos previstas, porque es de sumo interés, teniendo en cuenta la dimensión de lo que se acaba de plantear.

Muchas gracias.

El señor **VICEPRESIDENTE:** Muchísimas gracias.

Por el Grupo Popular, tiene la palabra la señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Gracias, señor presidente.

Quiero dar la bienvenida, en nombre del Grupo Popular del Congreso y del Senado, a don Carlos León de Mora, agradecerle su magnífica intervención y, además, tengo que decir, como gallega, que muy actualizada, porque hace escasamente un mes que el Tegra abrió las puertas en Santiago de Compostela. Sin lugar a duda, hay que agradecer también a Telefónica que haya apostado en su momento por ubicar los dos centros —uno en Galicia y otro en Valencia— para cuestiones relacionadas con la ciberseguridad.

Pocas preguntas nos quedan por hacer. Usted lo ha explicado de maravilla. Empezó con la anécdota del boli y la cinta y ahí me perdí, y ya me di cuenta de que, efectivamente, hay generaciones distintas en esta sala y la manera en que evoluciona el mundo *online,* que, como usted dijo, es acelerado y complejo. En el año 2004, las notificaciones a los diputados se hacían por fax —seguramente lo recuerda el presidente de la Comisión, que en aquella época era compañero conmigo—, llegábamos a casa el viernes y teníamos un fax en la bandeja diciendo que veníamos el martes. Esa era la forma de comunicación que teníamos para las sesiones de Pleno. Por tanto, ha cambiado totalmente. Por eso, me gustaría hacerle una serie de preguntas desde el punto de vista del estudio y de profesionales de la enseñanza, como es la cátedra que usted dirige.

Una es referida a si considera que el actual sistema de formación de profesionales en materia de ciberseguridad a nivel universitario es correcto. Después de lo que dijo creo que no, pero preferiría que me lo aclarase; si cree que sería deseable la creación de un grado en ciberseguridad, porque en este aspecto cada ponente nos dice que hay que hacer algo, pero necesitaríamos concretar. Yo propongo si puede ser un grado, o quizás considera usted útil o necesario mejorar el nivel profesional universitario de las profesiones relacionadas con la ciberseguridad industrial, o mejorar la formación profesional, que muchas veces es también la olvidada. Estamos hablando de algo muy técnico y a lo mejor, efectivamente, tenemos una buena canalización a través de la formación profesional. ¿Cuál es la vertiente que usted ve mejor? ¿Cómo evalúa las herramientas disponibles por el sector para la protección de la cadena logística a la hora de desplegar sistemas complejos, *smart cities,* por ejemplo, basados en dispositivos de bajo coste y fabricados en mercados sin el suficiente control de la calidad del software integrado? No sé si era usted o el anterior compareciente quien señalaba que tenemos que comprar toda tecnología a otras empresas, casi ninguna española y que dependemos de ellos. Hoy mismo el CNI decía que había firmado un convenio con Microsoft para mejorar los ciberataques, la ciberseguridad, es decir, dependemos de una empresa. ¿Hay una buena relación público-privada en materia de ciberseguridad? ¿Cómo evalúa la ciberseguridad de estos mismos dispositivos de bajo coste? El anterior compareciente comentaba acerca de un ayuntamiento que hacía dos anuncios sobre las cacas de los perros y de la Ley de protección de

cve: DSCG-12-CM-102

datos, de su aplicación en la Administración local. A lo mejor muchas veces no tenemos que ir al bajo coste, sino a lo más seguro. ¿Cree que los modelos de análisis de riesgo e impacto para la evaluación de este tipo de sistemas complejos se encuentran en el nivel de madurez adecuado?

Sobre formación y educación primaria, ¿debemos hacer algo en este nivel respecto a ciberseguridad? Francia, por ejemplo, lo tiene.

En cuanto a identidad, algún partido aboga por seguir con el anonimato; yo por la identidad digital, a mí no me preocupa lo que publico en mis redes y cómo lo publico porque no tengo miedo. ¿Debemos potenciar la identidad digital?

No sé si en su cátedra tienen algún dato sobre las injerencias rusas durante el 1 de octubre, si han hecho algún tipo de estudio. Como el gran comunicador a nivel de España, no sé si Telefónica tiene datos referidos a esos días y si se ha producido una mayor mención sobre temas de Cataluña desde el exterior.

Muchas gracias.

El señor **VICEPRESIDENTE:** Habiendo intervenido todos los grupos, doy la palabra al compareciente.

El señor **LEÓN DE MORA** (director de la Cátedra Telefónica Inteligencia en la Red y director del Grupo de Investigación Tecnología Electrónica e Informática Industrial (TIC-150) de la Universidad de Sevilla): Voy a tratar de ser breve, para que no acabemos demasiado tarde.

En primer lugar, quiero darles las gracias. Para mí ha sido un placer tener la oportunidad de comparecer y, además, les confieso que los que nos dedicamos profesionalmente al estudio, en el aspecto más amplio de la palabra, disfrutamos haciendo estas cosas. Les confieso que me lo he pasado bien preparando esta ponencia y he aprendido muchas cosas, por lo que para mí ha sido muy interesante.

En lo que tiene que ver con la aceleración de la tecnología y la capacidad, los sociólogos ya han detectado alguna cosa curiosa. Se ha producido un fenómeno de coevolución. El ser humano trabaja muy bien, es capaz de tomar decisiones en un entorno donde hay poca información, donde la información es vaga e imprecisa, y de una forma analógica, es decir, tomando una decisión detrás de otra. El mundo digital es completamente diferente: tenemos muchísima información, hay que tomar decisiones sobre muchas cosas a la vez y hacerlo en tiempo real. Esto a nosotros, a los que venimos del mundo analógico nos cuesta trabajo, obviamente. Seguro que casi todos ustedes tienen familia, tienen niños que están inmersos en lo digital desde que han nacido. Sorprendentemente, lo que los estudios demuestran y la experiencia también es que el ser humano ha evolucionado a ser capaz de trabajar simultáneamente con varias cosas. Ya nadie o casi nadie, a partir de cierta edad, ve solo la televisión; ve la televisión a la vez que está consultando el móvil y mirando no sé qué, o están trabajando en lo que en informática conocemos como multitarea. Se ha producido un fenómeno de coevolución, la propia evolución digital ha llevado a una evolución. Yo también lo noto, porque, al final, trabajo con gente joven —lo cual es una suerte, por cierto—, y los alumnos tienen mucha dificultad para concentrarse en un tema únicamente; tienen habilidad para manejar mucha información de forma paralela y les cuesta trabajo focalizar —después lo hacen— y dedicarse a un tema en concreto. Entonces, se están produciendo fenómenos que tienen que ver con la interacción de la tecnología en la sociedad que no tenemos todavía muy bien estudiados.

Tratando de responder a las cuestiones que me planteaba el señor Salvador, la formación —un tema que ha salido también en otras preguntas— es una cuestión compleja, y hay varios aspectos. Les diría que la demanda es asombrosa, pero no solo en ciberseguridad, sino en el ámbito de las tecnologías de la información. Hay facultades y escuelas de informática por todo el país, de telecomunicaciones y de otros aspectos que son coadyuvantes en este caso, y el problema con el que nos encontramos es que a nuestra puerta acuden los empleadores a buscar talentos y se pelean por él, literalmente. No sé si esto pasa en otros sectores —claro, yo estoy en este—, pero la pelea es constante: por favor, mándame los buenos a mí, y no se los mandes a este otro. O sea, si tuviera que recomendar —como me preguntaba— qué estudios, le diría que, en general, tecnología. Y también les digo que estoy en el mismo caso. A mi hija, que es muy buena estudiante y ahora empieza el bachillerato, le digo la palabra informática y se tira por la ventana. En fin, es verdad que hay una demanda cierta, pero también hay una labor que hacer, porque esto sigue asustando o sigue pareciendo algo árido. No sé muy bien cuál es la razón, pero es verdad que, como sociedad —y pasa en todas las sociedades occidentales, al menos— no somos capaces de acoplar las demandas que tiene el mercado de trabajo no con la formación, porque damos formación en todo, sino con la vocación. Es asombroso que se produzcan avalanchas de solicitantes, y el mundo universitario lo conozco bien, porque, aparte de mi trayectoria como catedrático y profesor de universidad, he sido vicerrector de mi universidad, además de CIO, y he estado encargado de una parte importante de lo que

cve: DSCG-12-CM-102

es el despliegue de títulos, y Sevilla es una universidad grande. Es verdad que somos capaces de dar mucha formación, pero el problema es que después no podemos obligar a los estudiantes a meterse donde de verdad ahora mismo hay oportunidades de empleo.

En cuando a su pregunta sobre los perfiles —he tenido que sacar de la presentación algunas transparencias porque era demasiado extensa—, pueden ver en esta el desarrollo de los perfiles que les comentaba antes. Es relativamente genérico. Por entendernos, uno es el que se sienta delante del ordenador, remangada la camisa, el que está directamente en el asunto, y otro tiene un perfil más de gestión. ¿Cómo llegamos a concretar esos perfiles? Me pedían en algún caso mi recomendación, que no iría por especializar mucho la formación en los grados, porque la tecnología cambia, y no sabemos a qué velocidad. Si nos detenemos en otra de las transparencias por las que he pasado un poquito rápido, pueden observar el hiperciclo de tecnologías de inteligencia artificial. Ahí están las principales tecnologías —que ya ven ustedes que son muchas—, y en un grado de madurez muy diferente. Las que están subiendo la pendiente son las que ahora están en expectativa y creciendo, las que están arriba son las que han alcanzado cierto grado de madurez, las que caen son las que parece que iban a prometer solucionar todos los problemas del mundo pero no es así, y las que vuelven otra vez a crecer son las que consiguen estabilizarse. Y esto cambia todos los años. Entonces, sin pensar en la necesidad de la empresa, porque, si uno piensa en la necesidad de la empresa, de la administración o del empleador, lo idóneo es que llegue alguien que se siente y en el minuto 0,0 sea ya productivo, se conozca la tecnología —pero eso es, como se dice en mi tierra, pan para hoy y hambre para mañana—, es mejor tener un perfil flexible, ser capaz de aprender, con una formación técnica sólida en el grado, y después utilizar el posgrado para especializarse.

Las universidades —voy respondiendo también a otras preguntas, al hilo de la formación— tenemos una gran autonomía a la hora de planificar nuestro mapa de titulaciones, es decir, no podemos quejarnos desde las universidades de que no tenemos la capacidad de adaptar la formación a las demandas de la sociedad. Ahora mismo hay procedimientos relativamente rápidos, sobre todo en el ámbito del posgrado —en el ámbito de los grados es un poco más prolijo—, y una universidad de un año para otro puede definir un título. Saben que los títulos oficiales se acreditan por la Agencia nacional de acreditación o la agencia autonómica correspondiente que haya consorciado con la agencia nacional, de modo que en dos años o año y medio puedo montar, entre comillas, un máster o un posgrado sobre un aspecto concreto de ciberseguridad. Esa posibilidad existe. Otra cosa es que exista la capacidad o que haya una demanda real de esa formación, pero las universidades pueden hacerlo.

En las enseñanzas medias, lo que sí demuestran todos los estudios es que los ciudadanos, en general, carecen de habilidades digitales. Una cosa es que se aproximen —sobre todo, ahora los chavales— a la tecnología de una forma muy cómoda. Pero la tecnología —y hablo también de mis hijos— no es solo jugar a la maquinita, sino saber moverse en un entorno digital, saber qué pasa con la información que pones ahí, los riesgos que tiene, saber manejarlo, saber que uno no puede hablar en el ámbito digital como se habla cara a cara porque se pierde la interacción personal, que uno no puede hablar en la red de lo que quiera impunemente, porque está identificado. Y ese es otro aspecto, porque existe la leyenda de que es muy difícil saber qué pasa, pero en Internet queda rastro de todo; con tiempo y con recursos se puede averiguar todo, incluso lo que está por debajo de la web, que es la web oscura. Es cuestión de que sepamos dónde mirar y determinar los recursos. Al final, no daremos con la persona física equis que ha provocado algún conflicto, pero probablemente demos con la ubicación física de la granja de trolls que lo ha hecho; eso sí se puede hacer. Por tanto, tenemos cierta sensación de impunidad, o los chavales, sobre todo —hablando de la gente más joven—, tienen cierta sensación de que es un mundo un poco de juguete, en el que no pasa nada, en el que todo es blanco. Sin embargo, queda un rastro, un rastro digital, otro problema con el que nos vamos a enfrentar también. Hoy en día cualquiera de nosotros tiene un rastro digital que queda indeleblemente dentro de la red. Y les aseguro que cuando se hace una entrevista de trabajo a una persona lo primero que se mira es su rastro digital, y si en esa trayectoria hay algo inadecuado, etcétera. Por eso, debemos ser conscientes de que tenemos una vida digital, una identidad digital paralela a la identidad física que estamos empezando a regular. Ciertamente, la regulación funciona a la velocidad que puede funcionar, pero hay unas zonas de grises que no están del todo aclaradas.

Me comentaba también el señor Salvador el tema de los ciberconflictos, uno de los temas que aparece en todos estos informes estratégicos, porque el problema no es ya que el ciberconflicto origine un perjuicio reputacional o de tipo parecido y quede en el ámbito de la red, sino que dentro de pocos años la

cve: DSCG-12-CM-102

ciberguerra puede ser la palanca que origine una guerra, pero una guerra con armas de verdad; eso está estudiado en los informes estratégicos. De hecho, hace poco leía unas declaraciones del presidente Putin, y decía que quien domine la inteligencia artificial dominará la sociedad en el futuro. O sea, esto es algo sobre lo que se está trabajando en esa línea. No hay convenciones, no hay un convenio, como existe de prisioneros de guerra —yo no soy un experto en esos temas—, pero en el ámbito digital es algo que hay que hacer y se es consciente de que hay que hacerlo, porque no es un mundo absolutamente impune.

Pasando a la intervención del señor Comorera, del Grupo Podemos, hacía alguna reflexión sobre el control de los datos. Hay una frase muy conocida que dice que el petróleo del siglo XXI son los datos. Ya lo ven, la primera petrolera en el ranking de capitalización bursátil, que antes era la primera, ahora es la séptima, y las seis primeras son empresas de datos, son empresas que no tienen activos físicos —no voy a decir ningún nombre, por no hacer propaganda—. ¿Donde está el valor de estas grandes empresas? El valor no está en su sede física, que son impresionantes —conozco alguna—, el valor no está en los activos ni en las sedes que tienen, el valor no está en las patentes que tienen, que ya tienen valor; el valor son las personas que allí trabajan y los datos que manejan. Y eso vale mucho más que una empresa tradicional eléctrica que tenga sus estaciones, redes y activos físicos. El dato es lo que va a mover la economía del siglo XXI. Los datos están por ahí, y no somos conscientes de adónde van los nuestros. Incluso, ya les digo que, conscientemente, en breve, no sé si muchos de ustedes pero les aseguro que mucha ciudadanía introducirá en su domicilio altavoces inteligentes, con tecnología de inteligencia artificial, que estarán escuchando todo lo que pasa en nuestro domicilio. Entonces, un día —lo he visto— le dará los buenos días al altavoz —así acabaremos— y el altavoz le dirá: me he enterado de que quieres hacer un viaje a no sé dónde y aquí tengo dos billetes, porque he conseguido en una oferta. ¿Cómo el altavoz sabe eso? Lo sabe por que tuviste una conversación con tu pareja en la que estabas comentando qué bueno sería ir a no sé dónde, y el otro estaba escuchando, agazapado. De hecho, se han dado casos de altavoces que han enloquecido, que se ponían a reír por la noche. **(Risas).** Sí, esto ha pasado. Incluso, hay algoritmos de inteligencia artificial que estos proveedores de datos han tenido que apagar. Estaban funcionando autónomamente a través de las redes y habían generado un lenguaje propio, un lenguaje autónomo, incomprensible para el ser humano, que les permitía comunicarse con sus otros congéneres. No quiero asustarles con un escenario del tipo Terminator ni cosas de esas, porque todavía la inteligencia artificial no tiene esas capacidades —esa sería una inteligencia artificial fuerte, una inteligencia artificial de propósito general, como tenemos los seres humanos, y eso puede que tarde décadas en conseguirse o a lo mejor no se consigue nunca—, pero las herramientas van avanzando, y, conforme ganen en autonomía y en capacidad, y, sobre todo, en capacidad de acceder a la información, algún susto pueden proporcionar.

En cuando a la cooperación público-privada, por mi experiencia y lo que puedo conocer, en general, en el ámbito tecnológico funciona extraordinariamente bien, o sea, hay una relación fluida entre los proveedores de servicios tecnológicos y las universidades. ¿Por qué? Porque, al final, como antes les decía, hay dos cosas: datos y talento. ¿Y dónde está? El talento, en general —también puede estar en otro sitio—, está estudiando en la universidad. Entonces, la oportunidad de acceder a ese talento de forma directa es un aspecto estratégico, porque lo que de valor puedan ganar esas instituciones será lo que le aporten las personas que a ellas se incorporen. Creo que es algo que está por explotar, y, cuando se explota y se establece una relación de confianza, funciona. Pero es verdad que somos dos mundos. Muchas veces los académicos estamos en una torre de marfil, pensando en nuestras cosas, mientras que los otros a lo mejor están en el día a día, pensando demasiado a corto plazo: hay que buscar un espacio de entendimiento. En ese sentido, las cátedras de universidad-empresa, como esta que tengo el honor de dirigir desde hace tiempo en el Universidad de Sevilla, son una especie de punto neutro, donde, sobre la base de mucha confianza, de estar trabajando, se reúnen gente de dos o tres ámbitos diferentes y de ahí surgen cosas. Una de mis preocupaciones es que mis alumnos reciban una formación adecuada y que sea la formación que necesita la sociedad, y, además, si puedo conseguir que tengan empleo, entonces hemos cerrado el círculo. Y este tipo de iniciativas funcionan bien. Por ejemplo, el tema del HackForGood comentado es algo que se hace a nivel nacional, porque es una red de veintitantas cátedras de universidad-empresa, y no solo es que se fomente el talento. También aparece el clásico hacker, ese que tenemos todos en la imagen cuando pensamos en él y que no voy a describir. Son tremendamente creativos, y se les reúne durante veinticuatro o cuarenta y ocho horas, pero lo interesante es que, aparte de que tienen unas ideas que son divertidísimas, en muchos casos a partir de esas ideas se han creado empresas y a partir de esas ideas se ha creado empleo, y la propia empresa matriz que lo fomenta los ha

cve: DSCG-12-CM-102

apoyado, los ha acompañado, los ha financiado hasta que han sido capaces de volar por sí mismos. Incluso, en algunos casos la idea o la empresa que se ha desarrollado se ha vuelto a incorporar. Tenemos varios casos de éxito. ¿Esto es una solución, como a veces parece que puede ser la solución mundial a todos nuestros problemas de empleo que tenemos como país? No, es aportar a una solución. Pero es verdad que en un aspecto muy concreto sí funciona muy bien y creo que es una experiencia que debería fomentarse.

Respecto a lo que comentaba el señor Raffo, sobre qué podría impulsarse desde el Gobierno, no es sencilla la pregunta, porque como bien les digo, en el ámbito de la formación reglada las universidades disfrutamos de bastante autonomía. Es verdad que cuando hacemos una propuesta de un título tiene que ser validado por la comunidad autónoma correspondiente, pero, en general, si uno presenta cosas sensatas, al menos en la universidad pública, que es la que conozco con más detalle y profundidad, y suelen ser títulos que están bien planteados, con unos recursos adecuados, etcétera, no suele haber problemas. Quizá deberíamos plantearnos alguna estrategia como país, como les decía, para orientar el talento hacia lugares que permitan una inserción laboral y una creación de riqueza, sin menoscabar otra formación de tipo humanístico, que, por supuesto, es necesaria. Por cierto, en todas estas fichas en las que se habla de temas de ciberseguridad y donde se determinan las profesiones, en todas ellas, aparte de las habilidades tecnológicas que se dan por supuestas, se habla de las *soft skills,* de las habilidades de comunicación, de trabajo en grupo, etcétera, y quizá debiéramos ser capaces de fomentar eso tanto en las enseñanzas medias como en la enseñanza universitaria.

Respecto al tema que me planteaba sobre qué pueden hacer los poderes públicos en cuanto a los sesgos, yo empezaría por vigilar nuestra propia casa. Si cualquier agencia, entidad, institución pública va a utilizar, y lo va a hacer —me refiero a que lo va a utilizar porque me consta que en algunos casos está en estudio y en otros se va a poner en producción—, algoritmos de este tipo que a partir de los datos son capaces de hacer un soporte de ayuda a la decisión, tendremos que requerir una información de cómo funciona aquello y en función de qué datos ha sido entrenado. Normalmente ocurre sin maldad, pero si uno dispone de un conjunto de datos que están sesgados hacia un determinado tipo de población, mujeres de determinada edad, etcétera, el algoritmo en sus decisiones va a estar sesgado hacia ese tipo de población. No es que el algoritmo sea maligno, porque no es ni bueno ni malo, no tiene moral, es lo que se le programa, con cierta autonomía para poder interpretar los datos. Ese riesgo de las cajas negras existe y, en mi opinión, habría que desarrollar algún tipo, no tanto, diría, de legislación, o quizá sí, como una serie de convenciones, por ejemplo, cuando a nivel público hacemos una compra de tecnología que especifiquemos que eso esté bien claro y definido.

A nivel global, ya les he dicho el número de líneas de código. El problema es que estos sistemas se autoprograman. Yo he programado sistemas de estos y uno se sorprende, por inesperadas, de las cosas que hacen. Muchas veces no eres capaz —este es un riesgo inherente a la tecnología— de explicar por qué se ha tomado esa decisión. De hecho, en todos los informes y en lo que tiene que ver con estrategias y temas fronterizos de investigación, una de las cuestiones candentes ahora mismo es cómo los sistemas de inteligencia artificial son capaces de explicarnos por qué tomaron una decisión.

Respondo ahora a la representante del Grupo Popular. Creo que he comentado antes lo del grado en ciberseguridad. Pudiera ser, tampoco pasa nada, pensando en el futuro de la persona, no en el mercado, que a lo mejor es interesante, que tenga un grado en ciberseguridad y sepa muchísimo de todas las técnicas *malwere* y de ciberdefensa y que al día siguiente esté parando ataques como un campeón, pero es verdad que se va a meter en un nicho. Me gusta que los estudiantes tengan una formación global, sólida, interdisciplinar, tecnológicamente fuerte, porque en poco tiempo, en meses, ese tipo de perfiles es capaz de adaptarse a la experiencia que necesite.

En cuanto a la seguridad en Internet de las cosas, la IoT, es un caso dramático. Les voy a contar un caso personal que sucedió en mi grupo de investigación la semana pasada. No voy a decir el nombre, pero era una empresa americana de nivel muy alto que vende unos dispositivos para el control de la red eléctrica utilizando tecnología de IoT. No era fácil de comprar, etcétera. Fue una cosa un poco compleja, pero al final llegó el dispositivo y las personas que trabajan conmigo en el grupo a los dos días vinieron con la cara blanca porque se les había ocurrido meter el *password* 1234 y no solo accedían a nuestros dispositivos, sino a los ciento cincuenta dispositivos que había por todo el mundo. Desde mi ordenador yo podía tirar una central eléctrica en Ohio. A ese nivel estamos. El nivel de seguridad de los dispositivos de IoT es mejorable. O se tiene en cuenta en el propio diseño de este tipo de dispositivos o después habrá que ponerles parches. Cuando el ámbito de las *smart cities* despliegue este tipo de soluciones, que va a

cve: DSCG-12-CM-102

ser explosivo, más con el tema que viene de *blockchain,* que permite eliminar mucha intermediación en transacciones entre máquinas, va a ser preocupante.

En cuanto a los modelos de análisis de riesgo, empiezan a verse atisbos de certificaciones. Todavía es un camino en el que es verdad que se está trabajando, pero la tecnología es tan cambiante y tan variada que es difícil. Sé que existe esa preocupación, y las empresas que emiten certificaciones de ciberseguridad tratan también de certificar sistemas, hay guías de buenas prácticas, etcétera, pero todavía falta hacer un recorrido. Estamos en el nivel estratégico, que es lo que les comentaba anteriormente de la cantidad de informes que están surgiendo entre los principales actores mundiales sobre hacia dónde va esta tecnología, sobre qué debemos legislar, qué nos debe preocupar, qué aspectos son clave, pero todavía no hemos aterrizado en el plano operativo.

Me ha preguntado por las injerencias rusas. De esto no sé absolutamente nada. Sería prudente comentarlo, pero en mi responsabilidad no he tenido ninguna información. Es verdad que tengo una relación fluida con Telefónica, pero no hasta el punto de saber si ellos tienen algún estudio hecho en este campo. Sí les digo que hay evidencias de que los Estados están continuamente al menos motorizando la red. Un porcentaje importante del tráfico de monitorización que existe en la red está llevado a cabo por los Estados, entiendo que dentro de sus potestades.

Creo que más o menos he conseguido contestar a todo lo que me han planteado.

El señor **VICEPRESIDENTE:** Muchas gracias, señor León de Mora, por su intervención y por sus aportaciones, que creo que han sido muy interesantes. Si hubiera alguna cuestión que pudiera contestarse por escrito o alguna aportación que quiera realizar, lo puede enviar a esta Comisión. También creo que se ha desgranado aquí alguna petición de comparecencia que se puede tratar en la próxima reunión de Mesa y portavoces.

Le agradecemos de nuevo su presencia.

A las cuatro tenemos la siguiente y última comparecencia. Como no ha llegado todavía, continuaremos a las cuatro. **(Pausa).**

— DE LA SEÑORA QUINTANA (PERIODISTA EXPERTA EN CIBERSEGURIDAD, AUTORA DE LOS LIBROS «CIBERACTIVISMO», 2012, Y «CIBERGUERRA», 2016, EDITORIAL CATARATA), PARA QUE EVALÚE LA SITUACIÓN ACTUAL DE LOS DERECHOS DE LOS USUARIOS DE INTERNET Y LAS SUPUESTAS CAMPAÑAS DE DESINFORMACIÓN QUE CONSTITUYEN SUPUESTOS CIBERATAQUES EN CONTRA DE ORGANISMOS PÚBLICOS Y PRIVADOS EN ESPAÑA. A PETICIÓN DEL GRUPO PARLAMENTARIO CONFEDERAL DE UNIDOS PODEMOS-EN COMÚ PODEM-EN MAREA. (Número de expediente del Congreso de los Diputados 219/000932 y número de expediente del Senado 715/000321).

El señor **VICEPRESIDENTE:** Continuamos con el orden del día, y damos la bienvenida a doña Yolanda Quintana a esta Comisión Mixta de Seguridad Nacional. Hemos tenido dos comparecientes anteriores que han realizado intervenciones muy interesantes, y estoy seguro de que esta será todavía mejor, si ello es posible, o por lo menos igual que la de ellos.

La señora Quintana es periodista, experta en ciberseguridad, autora de los libros *Ciberactivismo,* del año 2012, y *Ciberguerra,* del año 2016, editorial Catarata, y comparece para evaluar la situación actual de los derechos de los usuarios de Internet y las supuestas campañas de desinformación que constituyen supuestos ciberataques en contra de organismos públicos y privados en España. Evidentemente, debido a sus conocimientos, puede aportar aquellas cuestiones que considere oportunas.

La dinámica de la comparecencia es la misma que la llevada a cabo con el resto de los comparecientes. Habrá una primera intervención de la compareciente y luego cada grupo tomará la palabra por un tiempo de cinco minutos —una única intervención— para realizar las preguntas o exponer las cuestiones que consideren oportunas. Finalmente, volverá intervenir la compareciente.

Muchas gracias por su presencia y por su contribución a esta Comisión.

Tiene la palabra.

La señora **QUINTANA SERRANO** (periodista experta en ciberseguridad): Muchas gracias, señor presidente.

Buenas tardes, señorías. Gracias a todos los grupos parlamentarios, en particular al Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, que es quien ha propuesta mi

cve: DSCG-12-CM-102

comparecencia, por considerar que lo que puedo decir a sus señorías tiene interés para los trabajos de esta ponencia.

Debo decir, como anécdota, que no es la primera vez que tengo el honor de comparecer en el Parlamento. En el año 1997 tuve oportunidad de intervenir en esta misma sala, en la Comisión de Fomento, con objeto de la trasposición de la Directiva Televisión sin Fronteras, en calidad de experta en regulación de los medios y derechos de los usuarios. Como entonces, espero aportar lo que pueda a sus funciones legislativas y de control del Gobierno, así como a las conclusiones de esta ponencia, que es de gran interés por el contexto en el que nos encontramos.

Si me lo permiten, voy a empezar con dos citas que fueron usadas por el presidente de la Comisión de Libertades Públicas del Parlamento Europeo que durante seis meses estuvo analizando el espionaje masivo de los servicios de inteligencia norteamericanos —que la comisión consideró probados— y que viene muy bien para establecer los límites de los trabajos de esta Comisión y de mi propia comparecencia de esta tarde. Empezaba este informe del presidente de la comisión, un europarlamentario británico, con una cita de Hobbes que decía: La misión de un soberano, sea un monarca o una asamblea, consiste en el fin para el que fue investido con el soberano poder, que no es otro sino procurar la seguridad del pueblo. Es una cita, como ustedes saben, de Leviatán. Con esta cita de Leviatán de Hobbes sobre la obligación de los Estados de garantizar la seguridad de los ciudadanos, y otra del juez y jurista británico lord Bingham of Cornhill sobre la necesidad de no apartarse de los estándares que impone la sociedad democrática, arrancaba la exposición de este informe de la Comisión de Libertades Públicas. Esta tensión no es nueva en un entorno de ciberguerra, pero siempre que se va a regular la seguridad de los ciudadanos existe la tensión entre la seguridad y los Estados totalitarios que pretenden abarcar el ámbito de las libertades civiles y la obligación de los Estados democráticos como el nuestro de no apartarse de esos estándares internacionales de libertades y derechos humanos.

En mi exposición, por la brevedad del tiempo, me referiré a los libros que he publicado, que mencionaba el presidente en la presentación, y también a otras citas que incluyo en la documentación y que pueden ser de interés para sus trabajos y para las conclusiones finales. **(Apoya su intervención con una presentación en *Power Point).*** Me referiré a ellas brevemente. Me gustaría empezar, para contextualizar mi intervención, viendo de dónde partimos. Partimos de un contexto en el que hasta hace muy pocos años Internet suponía nuevas posibilidades para el activismo y para la comunicación sociopolítica. Ha permitido, de manera indudable, un mayor control y escrutinio de los poderes, y se pueden dar muchos ejemplos, como las plataformas colaborativas; un nuevo ecosistema informativo más rico, donde ya no están los actores tradicionales; nuevas formas de organización y movilización social, y se puede ver reflejada en esta viñeta la frase de los Estados autoritarios. La tentación de expulsar a los corresponsales para que aquello que todo el mundo esté mirando deje de hacerlo ya no es posible, porque cualquier persona con su móvil puede ser emisor de comunicación relevante. También hay nuevas formas de organización política y frente a las organizaciones y las movilizaciones sociales vinculadas a instituciones establecidas y jerárquicas. Vemos nuevas formas de organización basadas en movimientos de enjambre que se activan de manera puntual; por ejemplo, en un caso específico de *hacktivismo* puede ser el movimiento Anonymous, pero esto lo hemos visto en movimientos sociales de todo tipo.

El impacto de este tipo de fenómenos es indudable. De manera anecdótica, y como algo emblemático, podemos recordar que la figura del año en 2012 era el manifestante, y este manifestante relacionado con estas nuevas formas que permitía Internet. Estas posibilidades de nuevas formas de comunicar y nuevas formas de movilización social han creado de manera indudable una brecha entre dos ecosistemas que convivían y que no siempre se han entendido, por lo que esta convivencia no siempre ha sido pacífica. Se pueden citar muchos ejemplos, pero de manera anecdótica podemos ver esta declaración de un alcalde que consideraba que Internet podía ser el quinto jinete del Apocalipsis y con gran vehemencia invitaba a regular todos estos males que iba a traer este nuevo ecosistema digital.

Al mismo tiempo que existen estas nuevas potencialidades, que son indudables, que han traído las tecnologías, a favor de derechos de los ciudadanos, como el derecho a la información, el derecho de protesta, el derecho a intervenir en los asuntos públicos, han surgido amenazas que merman esta potencia. Por un lado, están los fenómenos de cibervigilancia global y las nuevas formas de censura que se apoyan en la tecnología, como los robots, y en el caso de otros Estados de América Latina como México están muy documentados; los ataques e intrusiones, los rastreos, el recorte de derechos y libertades, muchas veces con la intención precisamente de sofocar estas nuevas formas de activismo, de organización social. Por otro lado, en nuestra vida cotidiana dependemos de dispositivos y herramientas

cve: DSCG-12-CM-102

sobre cuyas aplicaciones tenemos muy poco control, por ejemplo, los dispositivos que empleamos para comunicarnos. Hay un entorno de ciberataques y ciberguerra que es cada vez más cotidiano. Junto a esto, está la ruptura de lo que venía a ser la primera enmienda de Internet, que era la propia arquitectura. Me permito reproducir la cita, porque es muy emblemática, de lo que era este entorno distribuido y abierto que suponían las tecnologías. La modalidad que encabeza esta lista de protectores de la expresión en el ciberespacio es una vez más la arquitectura, el anonimato relativo, la distribución descentralizada, múltiples puntos de acceso, ausencia de necesidad de ataduras geográficas, inexistencia de un sistema simple para identificar contenidos, herramientas criptográficas. Todos estos atributos y consecuencias del protocolo de Internet dificultan el control de la expresión en el ciberespacio. La arquitectura en el ciberespacio es la verdadera protectora de la expresión, constituye la primera enmienda del ciberespacio. Es una cita del famoso y mencionadísimo libro del *Código 2.0* de Lessig, como saben, uno de los padres de las licencias de código abierto y de compartir contenido en Internet.

En este entorno distribuido, abierto, en el que la arquitectura de Internet garantizaba todas estas posibilidades para los ciudadanos, también la ruptura de esta distribución, muchas veces relacionada con las propias herramientas que estamos utilizando empequeñeciendo Internet a pequeños nodos, y una realidad no solo cada vez menos centralizada sino más limitada, está rompiendo esa realidad tan favorable que yo dibujaba al principio. ¿Por qué debemos preocuparnos en ese entorno? Porque todo lo que tiene que ver con ciberataques y una situación de ciberguerra afecta, como se está viendo, a nuestros derechos y libertades, como han puesto de manifiesto comparecientes que me han precedido; indudablemente tiene consecuencias económicas; hay una cuestión de responsabilidad jurídica que en muchos casos no está clara y no está regulada; es una situación que ha dejado de ser excepcional —no me voy a detener en las estadísticas porque otros comparecientes las han actualizado—, porque podemos decir que el 65 % de los incidentes que se producen, según datos del Centro Criptográfico Nacional, que, a mi juicio, es la referencia estadística en esta materia, tienen un nivel de riesgo alto o muy alto. En los últimos años los incidentes se han multiplicado por diez. Además, nuestra relación con la tecnología ha variado. Tenemos dependencia tecnológica prácticamente para todas nuestras actividades en la vida cotidiana. Dependemos de aplicaciones y dispositivos que no controlamos y que utilizamos incluso para cuestiones muy sensibles, como operaciones financieras o comunicaciones sensibles, por ejemplo, de periodistas o representantes públicos.

Hay nuevas realidades. Ahí están viendo el mapa de un ataque masivo de negación de servicio en el año 2016 en el que se tumbaron, por decirlo de manera coloquial, es decir, quedaron accesibles las principales webs en todo el mundo, Twitter, Spotify, etcétera. Este ataque masivo al Internet de las cosas no estuvo producido, como venía siendo habitual hasta el momento, a partir del robo de redes zombis de ordenadores, sino de dispositivos conectados al Internet de las cosas. Fueron ataques de neveras, tostadoras conectadas a Internet de las cosas que previamente se secuestraron con un ataque de *ransomware*. Hicieron estas peticiones masivas contra estas webs. Hay nuevas realidades que son cotidianas en nuestros hogares y han aumentado la peligrosidad de ese entorno digital. Por no hablar de vulneraciones más críticas, como juguetes infantiles conectados también al Internet de las cosas que han sido objeto de ataques. Además, hay situaciones de mayor riesgo, como infraestructuras críticas, los ataques contra organismos e instituciones y determinados sectores sensibles. En todos ellos están documentados ataques en los últimos años.

Hay riesgos emergentes, viejas amenazas, como los ataques de negación de servicio que se actualizan con nuevas realidades, y todo esto tiene un impacto en nuestros derechos y libertades. Aquí voy a utilizar una anécdota que creo que puede ser muy gráfica, porque, a mi juicio, las cuestiones que afectan a nuestra seguridad no debemos dejarlas en manos de los técnicos. No sé si son capaces de identificar esta ilustración, pero causó muchos dolores de cabeza, también a los legisladores en esta casa. Esta es la imagen de un prion y era el mecanismo que iniciaba lo que se conoció como el mal de las vacas locas. Este prion generó una gran discusión, porque era una molécula cuya composición no se conocía muy bien, ya que estaba a medio camino entre la proteína y el virus. Los veterinarios dedicaron grandes esfuerzos a explicárselo a toda la sociedad. También comparecieron en esta casa, porque era un reto cómo afrontar legislativamente esta nueva realidad y esta nueva vulnerabilidad en el ámbito de la seguridad alimentaria. Sin embargo, al final, lo que había detrás de esto era un problema regulatorio. Había una forma de alimentación animal que no estaba ni en el ámbito de la Unión Europea ni en el ámbito de los Estados. Había una gran tensión entre intereses económicos, y estaban los ganaderos que empleaban una alimentación para el ganado que entonces era muy económica, que eran las harinas de origen animal, de donde procedía precisamente el prion. Había una necesidad de crear nuevas

cve: DSCG-12-CM-102

instituciones. A partir de esta crisis, en España se crea la Agencia Española de Seguridad Alimentaria, que es un organismo que en mis conclusiones propondré como ejemplo para nuevos organismos ante nuevos retos, porque crea un comité científico, crea la participación ciudadana y crea la intervención de los distintos ministerios afectados por el ámbito de la seguridad alimentaria.

Detrás de esta molécula tan compleja técnicamente —había un gran discurso técnico por parte de los veterinarios para explicarnos cuál era su origen y su verdadera naturaleza— lo que había era un debate social sobre cuáles eran los derechos de los ciudadanos, en crisis en ese momento, que eran la seguridad y la salud, qué intereses económicos habían propiciado que se llegara a ese momento, qué lagunas legislativas teníamos en España y en el marco de la Unión Europea de dispersión de competencias que no se estaban cumpliendo para llegar ahí, qué necesidad de medios existía para que las inspecciones fueran más eficaces. Por tanto, en el ámbito de la ciberseguridad y en el de la seguridad alimentaria hay que pasar del código del prion para ver realmente qué derechos están en juego y qué soluciones eficaces podemos adoptar para garantizar estos derechos.

Hemos pasado del código de un virus de seguridad informática al código de un virus informático. Este es uno de los virus que, a mi juicio, más daños ha causado en el ámbito de la ciberseguridad de Internet, que tiene una gran relación con la ciberguerra porque se le conoce como la primera arma digital. Fue un virus desarrollado. Años después se consideró acreditado por la empresa norteamericana Symantec que este virus estuvo desarrollado por Estados Unidos e Israel y atacó una central nuclear en Irán. No debemos quedarnos en el código del virus. Sin duda será muy apasionante saber cómo se consiguió programar, de hecho es apasionante cómo se programó, cómo se consiguió que una infraestructura crítica que está sin conectar a Internet, precisamente por razones de seguridad, se lograra infectar a pesar de este muro de aire. Esto pone sobre la mesa cuestiones que no son técnicas, que son las que yo quiero destacar en mi comparecencia. Supuso la primera acción ciberofensiva de unos Estados, en este caso Estados Unidos e Israel, y abrió la puerta a nuevas amenazas. Creó una gran alarma a la comunidad de ciberseguridad por la irresponsabilidad que suponía abrir el camino a nuevos tipos de ataques, que ya no solo iban a estar en manos de los Estados que lo habían desarrollado, sino de cualquier otro Estado o de cualquier otro operador en el ciberespacio.

Debemos preocuparnos no solo por no dejarlo en manos de los técnicos, sino también por cómo enmarcamos este debate. Esta cita que me gustaría compartir con ustedes del experto en seguridad Bruce Scheneier lo explica muy claramente. Si enmarcamos esta discusión de la ciberseguridad y la ciberguerra con una discusión de guerra, lo que se hace cuando hay una amenaza de guerra es llamar al ejército y tendremos una solución militar, si pensamos en estas amenazas en términos de delincuencia obtendremos soluciones policiales, que es a lo que se ha enfocado Internet. De hecho, hace dos legislaturas teníamos la subcomisión sobre redes sociales y su impacto en la infancia dentro de la Comisión de Interior. Ha sido un enfoque muy frecuente en la actividad de Internet. También hay que tener en cuenta que la forma en la que enmarcamos este debate —continuando con la cita—, la forma en la que hablamos sobre él, la forma en la que dan los titulares los medios de comunicación determina qué tipo de soluciones queremos. También la ciudadanía debe tomar parte y vigilar cuál es el enmarcado en el que se abordan los problemas de ciberseguridad y las soluciones que están dando los poderes públicos.

Los últimos datos de ciberamenazas en España —les dejo la documentación, porque no me voy a detener en ella—, cuáles son los ataques que están en auge, cuáles son las principales tendencias, etcétera. No me quiero detener en las estadísticas porque están en la documentación, están disponibles públicamente y otros comparecientes que me han precedido en los trabajos de esta Comisión ya les explicado. Mencionaré que según las conclusiones del Centro Criptográfico Nacional uno de los problemas es el espionaje masivo de los Estados; que faltan recursos, formación e instrumentos jurídicos, que es una tendencia compartida por todos los Estados que afrontan estrategias de ciberseguridad; que el mayor uso de herramientas, aplicaciones y dispositivos seguros se incrementa por una mayor sensibilización de los ciudadanos, ya que hay herramientas de cifrado y de correo seguro que cada vez son más cotidianas y ya no están en manos de actores sensibles. Estas tendencias se completan con las estadísticas que ya he dicho que les dejo en la documentación. Este sería el panorama del que partimos.

Ahora me gustaría centrarme en el motivo principal de mi comparecencia, en las conclusiones del libro *Ciberguerra*. Les voy a comentar cuáles serían las claves y por qué este tipo de conflicto presenta novedades frente a conflictos convencionales. En primer lugar, hay que llamar la atención sobre la complejidad del concepto ciberguerra, ya que no es un concepto pacífico y remitiéndome a la cita anterior tampoco es inocente cómo se quiera enfocar. Por ejemplo, este tuit de Associated Press, una de las

cve: DSCG-12-CM-102

agencias de información globales más importantes del mundo —no es un tuit falso, es un tuit que se posteó desde la cuenta oficial de AP en el año 2013—, decía: «Última hora: dos explosiones en la Casa Blanca y Barack Obama herido». Este tuit, que fue publicado en la cuenta de Associated Press con millones de seguidores y que es una referencia no solo para la sociedad sino para los medios de comunicación de todo el mundo, se había producido minutos después de que un redactor de Associated Press recibiese un correo electrónico. Este correo electrónico, supuestamente enviado por un funcionario de Naciones Unidas, decía: «Rápidamente lee este artículo que es muy importante» y se añadía una URL o un enlace a una página supuestamente del *Washington Post*. Como pueden suponer era un ataque típico de *phishing*. El atacante estaba teniendo el acceso a las credenciales de Associated Press, porque una vez que pinchó en este enlace se le abrió el cuadro de diálogo que le pedía el nombre de usuario y contraseña. Al periodista, como es habitual que los sistemas informáticos fallen, no le llamó la atención este paso intermedio y de esta manera estaba dando acceso a un grupo de atacantes que se conoce como el Ejército Electrónico Sirio y que fue quien posteó ese tuit que veíamos al principio. El tuit creó un gran terror en la población en los primeros momentos, al haberse supuestamente producido un ataque en la Casa Blanca difícil de verificar por aquellas personas que no se encontraban *in situ* en aquel momento. Este tuit creó una bajada en bolsa y creó lo que un ataque de terrorismo convencional, y no en el ámbito del ciberespacio, podría generar.

Este hecho, una vez que ya se aclaró cual había sido el origen del tuit falso y la agencia rectificó, creó el debate sobre si este tipo de acciones por parte de un actor exterior con el ámbito de crear el terror era una acción de ciberguerra. Por tanto, no es un problema pacífico porque es una realidad muy nueva con nuevos elementos, ni tampoco es un concepto pacífico porque depende —como lo veíamos con la cita Bruce Schneier— de cómo lo enmarquemos buscaremos determinadas soluciones o no.

Para intentar acotar, a pesar de esta complejidad y falta de consenso entorno al concepto, voy a resumirlo en cinco claves, que también los dos comparecientes que me han precedido en algunos casos han mencionado. La primera novedad de la ciberguerra es que sería aquel tipo de conflicto que, por un lado, se libra en el ciberespacio como forma específica, pero, por otro lado, también supone una prolongación de los conflictos convencionales. Hay muchos conflictos convencionales, pero prácticamente cualquier conflicto convencional hoy en día tiene su reflejo paralelo en el ciberespacio que presenta estas novedades. Por un lado, están los actores. En un conflicto convencional los actores son los Estados, en líneas generales cuando hablamos de una guerra clásica son quienes se enfrentan. Sin embargo, en la ciberguerra tenemos que tener en cuenta que hay muchos actores que están detrás de los ataques que se producen y de las ofensivas y que buscan determinada ventaja geopolítica. Por tanto, esta sería la primera diferencia. Como es la hora de la siesta, me he permitido una pequeña broma en la intervención.

Esta complejidad entre los actores que intervienen pone un problema sobre la mesa, que es el problema de la atribución: quién es el responsable que hay detrás de los ataques. Hemos visto antes que están los Estados, están los cibermercenarios, están los *hacktivistas,* están los ciberdelincuentes y están los cibervándalos, que solo hacen el mal por hacerlo, por llamar la atención sobre sus capacidades técnicas. Cuando hay un ataque, ¿cómo sabemos quién está detrás del ataque?

En la bibliografía que les he dejado al principio explico en líneas generales cómo se produce esta atribución desde el punto de vista de la ingeniería forense. Me gustaría destacar la propuesta de este académico del King's College de Londres, Thomas Rid, que es una referencia en la atribución de ataques informáticos. Normalmente los ataques se producen por un método de deducción, intentando acumular el mayor número de pruebas posibles en función de la hora en que se ha elaborado el código, el idioma que está detrás y que lo soporta. Sin embargo, esto no impide problemas en la atribución de los ataques, como pueden ser los ataques de bandera falsa. Es decir, como los atacantes saben cómo los informáticos forenses atribuyen el ataque es muy fácil hacer ataques que se conocen de bandera falsa, que son aquellos que van dejando migas de pan o pistas falsas para que el ataque se produzca contra un actor que no es quien realmente esté detrás de este ataque.

Hay otros problemas también, ya que al hacerse mediante un método de deducción no es una ciencia exacta, siempre hay datos que se pueden escapar y puede haber una intencionalidad detrás de ese ataque. Por tanto, para atribuir el ataque, y en la medida en que ustedes tengan que evaluar hasta qué punto es fiable una determinada atribución, les recomiendo la prueba y el método de este académico. Este profesor propone, por un lado, verificar cuál es el interés estratégico de este ataque, cuál es la operativa que ha seguido el ataque y si hay otros ataques previos que han seguido la misma operativa, y por otro lado, plantea también la parte más convencional, la parte táctica técnica, que es qué tipo de instrumentos

cve: DSCG-12-CM-102

y qué tipo de *malware* se ha usado para conocer qué otro atacante identificado previamente lo ha llevado a cabo.

El problema de la atribución de los ataques no es solo un problema técnico, que los académicos como Thomas Rid intentan solventar, sino que también hay un problema de partida ya que existen identidades difusas. Muchos atacantes en un entorno de ciberguerra, teniendo en cuenta que los Estados son el actor más peligroso y con mayor actividad según reconoce nuestro Centro Nacional de Inteligencia en sus informes anuales de ciberseguridad, muchas veces no dan la cara en su propia actuación. Ahí tenemos, por ejemplo, cómo la Unidad de Ciberataques de los servicios de inteligencia norteamericanos en muchas de sus actividades tuvieron el nombre de un grupo de *hackers* o un grupo de *crackers,* de atacantes informáticos, que hasta años después no se supo detrás que estaba vinculado con los servicios de inteligencia de un determinado Estado, en este caso de Estados Unidos.

Lo mismo ha ocurrido con los servicios de inteligencia de Rusia, donde también atacantes que se identifican durante años a partir de ataques a empresas concretas y que hacen tumbar webs, o que roban información, o que producen determinadas actividades en el ciberespacio, como fue el caso de Guccifer 2.0, el grupo de atacantes que se supone que está vinculado al robo de los correos electrónicos del Partido Demócrata norteamericano, más adelante se sabe que pueden estar detrás los servicios de inteligencia ruso. Por tanto, las entidades difusas es otro problema a la hora de atribuir la autoría o quién está detrás de un determinado ataque.

Un tercer problema es la lucha por el control político de las actuaciones. En el caso de Estados Unidos antes de crear el Cibercomando, que reside y está bajo los servicios de inteligencia norteamericanos (NSA), la ciberseguridad estaba bajo el Ejército del Aire; era el Ejército de Aire quien tenía las competencias de ciberseguridad en Estados Unidos. Curiosamente cuando se produjo el desplazamiento de competencias desde el Ejército del Aire a los servicios de inteligencia surgió una historia que se empezó a divulgar en los medios de comunicación, teniendo enfrente a la Wikipedia. Se empezaron a producir noticias de la historia de un virus, que se conoce como el mayor ataque informático en la historia del Ejército norteamericano.

Cuando vamos reconstruyendo la historia de atrás para adelante, que es lo que hizo en este caso en esta noticia la revista *Wired,* se llega a la conclusión de que es una leyenda urbana. Es decir, es una leyenda muy bien construida, ya que la entrada en la Wikipedia de este supuesto ciberataque masivo contra el Ejército estadounidense a partir de un virus está muy bien documentado, pero no hay pruebas que la hagan verosímil. La cronología de los hechos según se va filtrando informaciones sobre este ataque coincide con el desplazamiento de las competencias del Ejército del aire a los servicios de inteligencia norteamericanos en el ámbito de la ciberseguridad. Por tanto, la lucha por el control político de las actuaciones en materia de ciberseguridad también tiene su relevancia en las informaciones sobre ciberguerra.

¿Cuáles son las consecuencias de que haya múltiples agentes, de que el principal agente en el ámbito de la ciberseguridad y de la ciberguerra sean los Estados, que a veces estos Estados utilicen identidades difusas y que haya una complejidad de partida para la atribución de los ataques? Por un lado, tenemos que los Estados y esa actividad en el ámbito de la ciberguerra son uno de los responsables de la falta de seguridad del ciberespacio, como el caso de Stuxnet puso en evidencia; que no es el único caso cuando se crean armas para atacar una determinada infraestructura crítica como fue el caso de ese virus, sino que también cuando se recopilan vulnerabilidades de sistemas y de dispositivos informáticos para explotarlas de manera interesada por parte de los Estados, pero no se comunican a los fabricantes de estos dispositivos, al final ponen en riesgo a toda la comunidad internacional, como fue el caso de los ataques de *ransomware* que sufrimos hace unos años. Si rastreamos esos ataque para atrás tienen su origen en la filtración de unas ciberarmas, que en este caso eran una recopilación de vulnerabilidades que habían sido conseguidas por el equipo Equation que antes citaba y que estaba vinculado por los servicios secretos norteamericanos. Por tanto, no solo el desarrollo de ciberarmas por parte del Estado, sino también la recopilación de vulnerabilidades para explotarlas posteriormente suponen un riesgo como hemos visto en los ataques posteriores de *ransomware*. Aquí tenemos un mapa global con todos los países donde se han producido ciberataques, aprovechando estas vulnerabilidades que previamente los servicios norteamericanos habían recopilado para explotarlas en beneficio propio.

También tenemos las nuevas realidades ya que de hecho esta responsabilidad de los Estados fue objeto del Congreso Norteamericano de Ciencia y Tecnología, donde analizaron la implicación de ese tipo de armas y las lecciones que habían aprendido de ataques como WannaCry, teniendo su origen en la

cve: DSCG-12-CM-102

recopilación de vulnerabilidades por parte de los servicios de inteligencia. Por tanto, los Estados en su desarrollo de armas y de estrategias de ciberofensivas tendrían que tener en cuenta esta cita: «La gente que vive en casas de cristal —que es lo que somos las sociedades interconectadas— no deberían tirar piedras». Esta es una conclusión importante para tener en cuenta porque no podemos excluir si nuestro Estado está también desarrollando este tipo de armas, o en todo caso en su acción diplomática tendría que pedir cuentas a los Estados aliados sobre qué tipo de ciberarmas, tanto las que buscan un ataque ofensivo como pueden ser Stuxnet como las que recopilan vulnerabilidades para explotarlas posteriormente, nos pueden estar poniendo en peligro al resto de Estados y de sociedades.

También deberíamos llamar a la responsabilidad en este debate sobre la importancia del cifrado. Ataques como WannaCry o ataques en los que nuestras infraestructuras críticas pueden estar vulnerables deberían poner en evidencia, no solo porque Naciones Unidas dice que es un derecho humano, la importancia del cifrado. Y por no hablar solo de un Estado también tenemos que tener en cuenta que hay otros Estados como Rusia que está utilizando a Ucrania como un laboratorio para acciones de ciberguerra, llegando a provocar el apagón total de toda la población en un mes de diciembre con el daño que esto supone. Por tanto, las soluciones no tienen que ser individuales, tienen que ser globales, sabiendo el impacto y el daño que a toda la comunidad internacional pueden hacernos las acciones de ciberespacio de los distintos Estados.

Otro problema lo encontramos en los sistemas de cibervigilancia global. No solo estamos hablando de la pérdida de seguridad de nuestro entorno digital, por tanto, de nuestra vida cotidiana, de poder encender la luz, que fue lo que no pudieron hacer los ucranianos en el año 2016 con el ciberataque masivo de Rusia, sino que también están en juego nuestros derechos y libertades con los sistemas de cibervigilancia global de los Estados para ganar ventaja. No es algo que sea un mito, no solo lo ha acreditado el Parlamento Europeo sino que podemos ver figuras como el papa Francisco, que tiene la sabia precaución de poner una pegatina en la cámara de su iPad antes de dirigirse a los feligreses.

Otro problema también de estas acciones de cibervigilancia de los Estados es cuando a partir de ciertos ataques, como fue el caso del *hacker* Phineas Fisher que atacó a la empresa italiana Hacking Team, una empresa que desarrolla herramientas de espionaje, supimos quiénes eran los clientes de esta empresa Hacking Team. Muchos de ellos eran Estados autoritarios como Arabia Saudí y muchos Estados de América latina, pero entre los Estados que habían comprado herramientas de espionaje se encontraba España también, según esta información filtrada por este *hacker*. Hasta ahora tampoco hemos sabido por qué España compró herramientas de espionaje, qué uso se le dio y con qué tipo de cobertura legal —porque en ese momento no estaba aprobada la Ley de Enjuiciamiento Criminal que podía dar una cierta cobertura jurídica al empleo de estas herramientas— las compró. Por tanto, en esta primera clave, quiénes son los actores que intervienen y qué papel tienen los Estados, vemos que hay un gran número de retos y un gran número de responsabilidades en la actividad de los Estados.

Voy a ir rápido, las siguientes son más sencillas. Nos encontramos en un nuevo campo de batalla que es el ciberespacio. No me voy a detener en este tema porque el compareciente de esta mañana ya lo ha mencionado, pero no pueden establecerse capas distintas entre el mundo virtual y el mundo real. Estamos en tres capas interconectadas, estamos en una guerra en red que sería otra novedad. La ciberguerra es una guerra asimétrica, en la que no hay un solo frente y donde se emplean tácticas atípicas. Es una guerra en la que hay nuevas formas de ataque y nuevas armas y objetivos, y también por tanto nuevos retos regulatorios con armas autónomas y con el empleo de la inteligencia artificial. El uso de estas armas representa un gran reto para los reguladores y para toda la ciudadanía. Además hay nuevas tácticas, ya que si en la guerra convencional podíamos entender que era una guerra de posiciones y la geometría sería la técnica que permitiría ver los avances, ahora tenemos otras técnicas como son los grandes datos que también ponen en juego nuestros derechos y libertades.

Yo cité al principio en las referencias bibliográficas, entre otros, un libro de reciente aparición titulado *Armas de destrucción matemática*, donde se revela cómo los grandes datos al final están condicionando y suponen un contexto totalitario que puede vincular desde lo que paguemos en nuestro seguro de coche, a si podemos entrar en un determinado país. También tienen que ver con la ciberguerra, porque muchos de los ataques que se están produciendo por armas automáticas, la determinación de un determinado objetivo se realiza de manera predictiva a partir de técnicas de *big data*. Por tanto, este nuevo tipo de técnicas también suponen un reto en el nuevo entorno de ciberseguridad y ciberguerra. Hay nuevas formas de ataque que aquí les enumero, pero no me voy a detener más porque ya les han hablado de ello en otras comparecencias previas.

cve: DSCG-12-CM-102

Además, como forma de ataque en una guerra asimétrica las acciones de propaganda, desinformación y el uso de manera interesada de ciertas desinformaciones tienen un gran peso en la sociedad civil. También lo hemos visto aquí y ha centrado buena parte de los trabajos de esta Comisión. Este nuevo entorno ha saltado a la agenda de los legisladores de todo el mundo. En el caso de España no es algo ajeno, de hecho se ha aprobado también alguna proposición no de ley por parte del Congreso de los Diputados y otros Estados como Alemania, Francia y Reino Unido también han iniciado esta senda regulatoria para intentar atajar esta pata de la ciberguerra, como serían las actividades de propaganda y desinformación basadas en ataques y el robo de información sensible.

Las conclusiones que me gustaría transmitirles es que en un entorno digital en el que los emisores tradicionales, como veíamos, habían perdido el monopolio del discurso político o de creación de la libertad, regular Internet es inevitablemente una tentación como forma de regular el flujo informativo. Frente a ello entidades como la Plataforma en Defensa de la Libertad de Información y Medios de Comunicación han publicado que aquí —lo ha citado el otro compareciente— el manifiesto en defensa de la libertad de información. La forma de intervenir frente a estas acciones de propaganda no puede ser intervenir y limitar el libre flujo informativo, a la vez esto debe de ser compatible con garantizar un espacio público digital fiable, transparente y responsable, transparente por parte de todos los actores, incluidos los actores tecnológicos que intervienen en este flujo informativos. Por tanto, la transparencia por ejemplo de los algoritmos es una condición fundamental. Estos retos, la necesidad de garantizar un ecosistema informativo fiable, pero a la vez, mantener como veíamos en las citas con las que yo empezaba la comparecencia, los límites de un sistema democrático se encuentran conciliados a nuestro juicio en documentos como la Declaración conjunta de los relatores sobre la libertad de expresión en esta materia.

A nuestro juicio las medidas que se están planteando en ocasiones por parte de algunos grupos parlamentarios, pero, sobre todo, aquellos países que ya han aprobado medidas como pueden ser Alemania, Francia o Reino Unido pueden atentar al derecho a la libertad de expresión e información. No es una opinión que mantenga a título personal esta compareciente, sino que los relatores de Naciones Unidas y la OSCE han llamado su atención sobre este riesgo y la propia Comisión Europea en sus conclusiones también advierte sobre la no conveniencia de regular en esta materia.

Al mismo tiempo, este tipo de conclusiones no están sustentadas en un conocimiento científico solvente. Muy recientemente cuando se aprobaba precisamente esta proposición no de ley se citaba un estudio que en esos días se había difundido en los medios de comunicación, que decía que las noticias falsas tenían un mayor alcance que las noticias verdaderas. El problema de la conclusión de este estudio, como otros que se están poniendo sobre la mesa, en apoyo del posible impacto de las campañas de desinformación en procesos electorales es su falta de rigor metodológico. Por un lado, en este caso las hipótesis serán muy incompletas. No se trataba de medir el alcance sino el efecto real de ese alcance en las decisiones de voto o en los procesos de formación de opinión pública de la ciudadanía. Por tanto, una cosa es el alcance de las informaciones y otra cosa es el impacto que realmente puedan tener esas informaciones en lo que preocupaba el legislador en ese momento, que era el proceso de decisión de voto o de formación de la opinión pública.

Además, son soluciones simplistas porque son fenómenos complejos, como seguramente sus señorías comparten conmigo y también como otros comparecientes han puesto sobre la mesa. Aunque sea periodista no podemos olvidar, por ejemplo, en el caso de Estados Unidos el papel imprescindible que jugaron los medios de comunicación, llamando la atención sobre determinados fenómenos justamente en los momentos antes de que se fuera a producir la votación. Por tanto, son fenómenos complejos en los que intervienen todos los actores, no solo el atacante sino todos los actores que están en el ecosistema informativo y todo esto hay que tenerlo en cuenta.

Para finalizar, y no irme demasiado de tiempo ni abusar de su generosidad, mencionaré las principales tendencias y retos que tenemos. Hay nuevas campañas y nuevas ciberofensivas que tenemos que tener en cuenta, no solo los ataques convencionales sino que también comparto la preocupación que tienen sus señorías sobre las campañas de intoxicación y propaganda. Hay una tendencia y hay un reto que no podemos olvidar, donde yo he puesto la atención porque creo que lo merece, que es ser conscientes de los actores con una mayor capacidad de ataque, que no son siempre los ciberdelincuentes o los *hackers* como este concepto que se tiende a difundir, sino que los Estados son fundamentalmente hoy por hoy el actor más peligroso en el ciberespacio; que hay que tener en cuenta los daños colaterales de las operaciones de ciberguerra, como se puso en evidencia con los ataques de WannaCry o Petya, que tenían el origen en acciones de ciberofensivas de un determinado Estado; que el espionaje masivo de los

cve: DSCG-12-CM-102

Estados, a pesar de las condenas de prácticamente todas las instituciones de derechos humanos y en nuestro caso del Parlamento Europeo, vulneran los derechos civiles.

Aprovecho para pedir de manera expresa que esta ponencia incorpore a sus conclusiones este informe del Parlamento Europeo, que recoge un catálogo de recomendaciones a los Estados miembros en materia de ciberseguridad y en materia de ciberespionaje para garantizar los derechos y libertades de los europeos. No hay ningún Estado miembro, que me conste, que lo haya llevado a la práctica. Por tanto, este trabajo de los parlamentarios europeos durante seis meses debería incorporarse a mi juicio, y así se lo solicito y se lo sugiero, a las conclusiones de esta ponencia para que se aproveche este trabajo, en lo que tiene que ver con ciberseguridad y ciberespionaje, que han hecho ya los legisladores comunitarios.

En cuanto a acciones defensivas o preventivas, a pesar de la mayor sensibilización, faltan recursos y formación —coincido con el ponente que me ha precedido esta mañana, con David Maeztu—. Los recursos no solo deben darse al Ejecutivo o a los órganos de la Administración competentes en garantizarnos la ciberseguridad, sino también al Poder Judicial y también hay que hacer campañas de sensibilización hacia los ciudadanos.

Antes de terminar con las recomendaciones quiero hacer una última cita de David Casacuberta, uno de los pioneros en el ciberactivismo que también compareció en el Senado en los años noventa cuando el Legislador español intentaba regular este entorno distribuido, caótico que es Internet. Recientemente decía David Casacuberta: «Internet no es una tecnología, Internet es lo que dice Lessig, es una Constitución. Es una serie de conceptos que se ponen en juego y que podían ser muy diferentes. Si nos creemos que la Red es libre porque es imposible que los Gobiernos la controlen porque es una tecnología, estamos engañados». En este contexto a mí me gustaría que mis recomendaciones fueran en esta línea de recuperar un Internet en la medida en que un Estado todavía pueda hacerlo, un Internet distribuido abierto, seguro y que garantice los derechos de los ciudadanos.

Por tanto, mis recomendaciones, peticiones o sugerencias a sus señorías serían las siguientes. En cuanto a derechos y libertades a mi juicio creo que deben recuperarse las libertades recortadas en los últimos años con la coartada de la seguridad. Es tiempo para ello, el próximo 1 de julio se cumplen tres años de la entrada en vigor de la reforma del Código Penal. Este Código Penal de manera muy grave penaliza Internet como tal canal. Hay que tener en cuenta que puede tener más riesgo escribir un tuit con doscientos seguidores, que lanzar un mensaje en televisión. De hecho hemos visto a tuiteros que han pasado por la Audiencia Nacional. Afortunadamente algunos han sido absueltos, pero por haber hecho un tuit en cuentas con muy poquitos seguidores. Por tanto, el canal no tiene que estar criminalizado, sino el mensaje en sí y a partir de los criterios restrictivos y muy restrictivos que dicta Naciones Unidas, sobre todo para delitos de terrorismo. Por tanto, urge descriminalizar Internet, como se ha hecho en la última reforma del Código Penal.

En cuanto a cibervigilancia y rastreo reitero mi petición de que las conclusiones del informe del Parlamento Europeo se incorporen a las conclusiones de esta ponencia. La estrategia de ciberseguridad se debe dotar, siendo un buen mecanismo el que tiene España en cuanto a que coordina competencias y establece muy claramente los distintos niveles de responsabilidad, de medios y se debe de guiar cualquier decisión en materia de ciberseguridad por el conocimiento técnico independiente y también por la transparencia. Abogo por el modelo que se sigue en seguridad alimentaria con un comité científico independiente que establece el nivel de riesgo y las necesidades regulatorias y también con transparencia, cualquier persona se puede meter en la página de la Agencia Europea de Seguridad Alimentaria (EFSA) y ver sus dictámenes sobre qué riesgo hay, dónde no hay riesgo y qué necesidades hay de regularlo. Por tanto, conocimiento independiente y transparente en estas conclusiones.

Respecto a transparencia y derecho a la información la trasposición de la Directiva sobre Seguridad de las Redes no solo debe establecer la responsabilidad de los actores económicos y privados, sino también las obligaciones de transparencia. Seguramente si una entidad financiera o una compañía eléctrica sufren un ataque en España no les será plato de buen gusto ser transparente en ese ataque. Sin embargo, es un derecho de los ciudadanos y también como hemos visto en el caso de seguridad alimentaria ser opacos en la información al final supone una crisis de confianza en los ciudadanos y un mayor coste económico. Por tanto, se debe aprovechar la trasposicion de esta directiva para establecer claramente las obligaciones de transparencia de los operadores económicos que sufran ciberataques.

El derecho a la seguridad de la ciudadanía es el mismo que tienen los consumidores y usuarios respecto a cualquier producto o servicio. Por tanto, en la responsabilidad jurídica en el Internet de las cosas debe extenderse la responsabilidad que tiene cualquier fabricante de un producto o servicio

cve: DSCG-12-CM-102

actualmente en nuestro país en el marco de la Unión Europea porque la normativa de consumo es comunitaria.

En cuanto a protección de datos y derecho a la información lamentablemente ayer conocimos una sentencia del Tribunal Constitucional, que esperamos que en un futuro sea matizada por el Tribunal Europeo de Derechos Humanos, que establecía que los buscadores de las hemerotecas digitales de los medios también estaban sujetos al derecho al olvido. Esto supone que una persona de interés público, porque por eso ha aparecido en un medio de comunicación porque ha sido noticioso, pueda ejercer su derecho a que no aparezca en el buscador y su nombre no sea un criterio de búsqueda en las hemerotecas de los medios. Creemos que los trabajos legislativos que ahora se están llevando a cabo para reformar la Ley de Protección de Datos puede ser una buena oportunidad, y así se lo solicito a sus señorías, para excluir a los buscadores de los medios de comunicación del derecho al olvido. Del mismo modo hay otros derechos digitales en juego, no solo en el ámbito de la ciberseguridad. También en estos días en el ámbito europeo se está discutiendo la Directiva de *copyright* y en esta tensión que yo mencionaba antes de dos mundos que conviven pero no se sincronizan, el mundo analógico y el mundo digital, tenemos una directiva de *copyright* que supone una gran vulneración de derecho a la información.

Por último, en cuanto a las estrategias de desinformación hay que remitirnos a los informes de la Comisión Europea y los relatores de derechos humanos. No puedo evitar mencionar que hoy dos periodistas que han comparecido ante los juzgados para informarles de que han interpuesto una querella contra ellos, Ignacio Escolar y Raquel Ejerique de *ElDiario.es*. Hay que tener en cuenta que las filtraciones no solo han sido un elemento que han merecido el Premio Pulitzer, que es el premio de periodismo más prestigioso del mundo, sino que ante la opacidad de los poderes y de determinados operadores, como puede ser el caso de las filtraciones, de las evasiones fiscales o los papeles de Panamá, las filtraciones es el único medio para que la ciudadanía tenga acceso a información relevante que permanece oculta y a determinadas irregularidades. A instancias y por impulso del Grupo Parlamentario Ciudadanos ahora se está tramitando en la Comisión Constitucional una proposición de ley de protección al denunciante. A nuestro juicio esta proposición de ley sería el espacio legislativo en el que se deben proteger también las filtraciones y a aquellas personas que han realizado una intrusión o un acceso, con determinadas cautelas, a un sistema informático que ha permitido de esta manera sacar a la luz datos relevantes como pueden ser los papeles de Panamá.

Muchas gracias. Les agradezco sobre todo su paciencia.

El señor **VICEPRESIDENTE:** Muchas gracias.

Tiene la palabra el señor Gutiérrez.

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

Muchísimas gracias, señora Quintana, por su exposición. Le doy la bienvenida en nombre de mi grupo parlamentario a esta Comisión, y, en nombre de mis compañeros, que seguramente lo repetirán, a esta casa, que, como usted ya bien conoce, también es la suya.

Ha sido una exposición muy interesante, larga pero creo que precisa, porque era amplia en la cantidad de conocimientos que quería transmitirnos. He anotado unos cuantos temas para hacerle algunas preguntas.

Se ha referido usted a recursos, instrumentos legales y formación. Lógicamente, a esta Comisión han venido otros comparecientes, no solo en el día de hoy, y hemos tratado estos temas. Hemos hablado de la falta de recursos por parte de la Administración, de la dificultad en muchos casos para proporcionar recursos en esta prevención a aquellos que son más vulnerables, que son los usuarios finales, las pymes y los autónomos, a quienes, les cuesta muchísimo más dedicar recursos que a la propia Administración del Estado, a la que digamos que siempre le resulta más fácil, y lo mismo sucede con los temas de formación. Pero en cuanto a la parte legal, por ser la que a nosotros nos compete más, me gustaría que incidiera en los instrumentos legales. Se refería usted a la protección, y justo en la comparecencia anterior nosotros lo habíamos propuesto precisamente para defensa de aquellos profesionales que se dedican al *hacking* ético, porque creemos que es una medida muy importante en la prevención. Al final, tenemos que hablar de prevención si estamos expuestos a un ataque, a una guerra, y entonces hay que actuar de otra manera. Pero ese es otro discurso, que para mí es diferente y entra en otros ámbitos que la Administración también debe conocer y controlar, aunque creo que lo está haciendo de forma eficaz. Me preocupa mucho más el tema del vulnerable, que es la sociedad, en general, el usuario, el consumidor final, que son

cve: DSCG-12-CM-102

precisamente aquellos que tienen menos medios. Por tanto, quisiera que usted nos detallara algo más qué instrumentos legales le parecen mejor.

Creo que ha olvidado tratar una pequeña parte, aunque lo ha mencionado de pasada, y es una amenaza grande. Me refiero al propio mercado que existe ya hoy en día y al que los Estados acceden a comprar armas. Igual que uno compra aviones, fragatas o pistolas automáticas, hay un mercado de las ciberarmas, y creo que ahí hay un tema que a nosotros nos falta por regular, porque es un delito que no existe en nuestro ordenamiento jurídico. Está un poco relacionado con lo que he comentado antes.

Me han surgido dos dudas, una en cuanto a la participación o colaboración que deben tener aquellas grandes empresas que dan soporte a nuestras infraestructuras críticas, que han de ser transparentes, y creo que lo son. De hecho, FNPI trabaja eso, y son transparentes con la Administración. Pero no sé si tiene mucho sentido que sean transparentes con todos los usuarios. Personalmente, cuando enciendo la luz no me aporta mucho saber si Iberdrola ha tenido 327 o 257 ataques. Creo que acabamos generando una especie de síndrome permanente por sentirnos atacados y vulnerables y que a veces hay que proteger a la propia sociedad ante un exceso de vulnerabilidad o información. Lo digo entre paréntesis.

Por otra parte, me ha parecido entender que usted esperaba que esto se solucionara un poco por la parte buenista de los Estados, que no deben atacarse. No sé si no le he entendido bien, pero me ha parecido que usted decía algo así como que los Estados deben firmar códigos éticos en los que se comprometan a no atacar a otros Estados. Me parece muy difícil, porque el ciberataque no es más que la guerra por otros canales distintos de los que se venían empleando. Pensar en estos momentos, en el siglo XXI, que los Estados no van a atacarse unos a otros, y no me refiero a un ataque puramente militar, porque hay ataques económicos, como los aranceles, etcétera, no deja de ser un juego en el que todos los Estados estamos imbricados.

Muchísimas gracias. Nuevamente le felicito por su exposición y le agradezco este tiempo que ha compartido con nosotros.

El señor **VICEPRESIDENTE:** Muchas gracias.

Tiene la palabra el señor Comorera.

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

Muchas gracias, señora Quintana, por su extensa exposición.

Me gustaría insistir en el tema, porque en esta Comisión se ha analizado el fenómeno de la desinformación y nosotros creemos que se da de forma interesada una confusión que entendemos grave, que es equiparar en cierta medida los conceptos de ciberguerra y desinformación, que en nuestra opinión son distintos. Por eso, le pregunto si es un error equiparar los conceptos de ciberguerra y desinformación.

Por parte del anterior Gobierno hubo anuncios de crear algún órgano para controlar la desinformación, al estilo de un ministerio de la verdad. Le pregunto si no sería peligroso para la libertad de expresión y para el derecho a la información que sea un Gobierno el que decida qué información es falsa y cuál no.

Aunque es un problema que hay que abordar, sin duda hasta ahora no se ha demostrado que España haya sufrido una alarmante epidemia de noticias falsas. Al contrario, un primer análisis independiente en Europa del Instituto Reuters y la Universidad de Oxford desacredita el discurso político alarmista que se ha desatado en torno a este fenómeno. Dice este análisis que las *fake news* han tenido un alcance que no llega al 1 % de los usuarios de Internet. Asimismo, el Centro Criptológico Nacional, que entre sus funciones tiene la de garantizar la seguridad de las tecnologías de la información, confirmó que no se detectaron ciberataques del Gobierno ruso ni de otro Estado durante la llamada crisis catalana. A pesar de eso, en esta misma Comisión hemos oído acusaciones, sin pruebas, sobre esa injerencia. Sobre el hecho de incluir la desinformación como una amenaza, por ejemplo, en la nueva estrategia de seguridad nacional, ¿cree que la aplicación de medidas para luchar contra esta amenaza puede desembocar precisamente en medidas que vayan a poner en riesgo la libertad de información y de expresión?

Hablaba usted de soluciones, de cuáles queremos. Me gustaría que nos diera su opinión sobre cuáles debemos querer. No me ha quedado muy claro, según su idea, qué soluciones necesitamos.

Respecto a los recursos, quisiera conocer su opinión sobre la inversión que se está haciendo en España en materia de ciberseguridad si nos comparamos con otros países que tienen mucha más inversión, como podrían ser Estados Unidos, Reino Unido o Israel.

También le preguntaría si sabe si hay injerencia o intereses privados en el fenómeno de la desinformación.

Muchas gracias.

cve: DSCG-12-CM-102

El señor **VICEPRESIDENTE:** Gracias.

Por el Grupo socialista, tiene la palabra el señor Álvarez.

El señor **ÁLVAREZ VILLAZÁN:** Gracias, señor presidente.

Muchas gracias, señora Quintana, por la exposición que ha realizado. Quizá se necesitaría mucho más tiempo para todo lo que nos podría haber dicho, pero el tiempo es el que es.

Me gustaría comenzar diferenciando los dos aspectos fundamentales que deduzco de su intervención y que creo que también se reflejan en *Ciberguerra,* el libro que ha escrito usted. Me refiero a la diferencia entre lo que supone para los Estados y las grandes empresas estas nuevas amenazas *online* y lo que suponen para los ciudadanos, que me preocupa todavía más, sobre todo por la desprotección que pueden tener cuando no son conscientes de este problema que les afecta, lo que les impide defenderse de las vulnerabilidades de este siglo. En su libro se dice que en una guerra la primera víctima es la verdad. Me ha llamado la atención, porque lo comparto totalmente y es lo que más me preocupa. Creo que englobaría todo el planteamiento que estamos haciendo. Si la primera víctima es la verdad, tenemos realmente difícil la tarea de podernos defender. Cuando falta información veraz, cuando partimos de informaciones que pueden ser falsas, es muy difícil defendernos de esas amenazas.

Me preocupan los distintos informes que se nos han venido dando. Por ejemplo, no hace mucho Joaquín Castellón, director operativo del departamento de Seguridad Nacional, advertía de que podemos estar preparados en nuestro país para un ataque convencional pero que realmente no estamos ni en los cimientos tan siquiera para poder construir algo que nos defienda de los ataques relacionados con la ciberseguridad. Teniendo en cuenta estas declaraciones, me preocupa que los tres principales organismos que tenemos en nuestro país, el Incibe, el Centro Criptológico Nacional y el Mando Conjunto de Ciberdefensa, no dispongan de la preparación necesaria para poder afrontar estas nuevas amenazas, y más cuando los propios servicios del cibercrimen de la Policía Nacional y de la Guardia Civil coinciden en que los incidentes que están ocurriendo, que son numerosos, no son todos los que realmente se producen, porque muchos afectados ni siquiera lo denuncian. Por recordar datos que se han dado también en otras comparecencias, el Incibe pasa de registrar 18 000 casos en 2014 a 120 000 en 2017. Si tenemos en cuenta los informes de la Guardia Civil y de la Policía Nacional acerca de que no son todos los que se producen, desde mi punto de vista realmente es una situación muy muy preocupante.

Acerca de la desinformación, las noticias falsas y la influencia de este tipo de noticias en la población, creo que todos llegamos a la conclusión de que es necesaria una regulación. He creído entender que tiene usted cierto recelo a que la regulación pudiera ser excesiva y afectara también a la libertad de expresión. Teniendo en cuenta que esa preocupación puede ser razonable, me gustaría preguntarle si no cree que realmente es necesario poner todo el empeño. Que la regulación tiene que ser inteligente, por supuesto. Que tiene que ser racional, por supuesto. Pero quizá habrá que sacrificar algunos de los aspectos relacionados con la libertad de expresión, teniendo en cuenta que hay quien la está utilizando para transmitir informaciones faltas.

Por último, me gustaría preguntarle si cree que la directiva NIS, de seguridad en redes y sistemas de información, de la Unión Europea, puede suponer una solución o un primer parche para evitar este tipo de desinformaciones que se vienen produciendo.

Me gustaría hacer más planteamientos, pero comprendo que el tiempo es el que es y creo que tenemos bastante con lo que estamos avanzando. Muchas gracias.

El señor **VICEPRESIDENTE:** Se lo agradezco.

Por el Grupo Popular, tiene la palabra la señora Marcos.

La señora **MARCOS DOMÍNGUEZ:** Muchas gracias, señor presidente.

Muchas gracias, señora Quintana.

Una cuestión previa, para al *Diario de Sesiones,* porque a veces se escuchan cosas que no deben quedar sin respuesta. El Gobierno anterior en ningún momento ha coartado ninguna libertad, ninguna. Lo que ha intentado —y es la obligación de cualquier Gobierno democrático— es que se cumpla la ley, porque, como usted sabe o entiendo que debería saber, sin ley no hay libertad ni hay fácilmente convivencia.

Señora Quintana, en el ejercicio de su comparecencia como experta en ciberseguridad, usted sabe que estas comparecencias son para preparar un informe sobre ciberseguridad y me gustaría que nos aclarara algún aspecto que ha comentado al referirse a la Estrategia de Ciberseguridad que se aprobó en 2013 y que se ha ido actualizando en el capítulo anual de la Estrategia de Seguridad Nacional. Ha

cve: DSCG-12-CM-102

dicho usted que faltan medios, un conocimiento técnico independiente y transparencia. Querría que nos aclarara qué medios son los que faltan, qué problema hay en cuanto a conocimientos técnicos que no existan o no sean independientes, cuáles son, y cuál es la transparencia que también usted echa en falta. De paso, querría que nos comentara cuál es su opinión, cómo valora el papel del Incibe, cómo valora el trabajo de Red.es, cómo valora la tarea que realiza el Consejo Nacional de Ciberseguridad, si le parece que cumple esas garantías de conocimiento, medios y transparencia, y, finalmente, qué sugeriría usted al nuevo Gobierno, al Gobierno que se puso en marcha el día 2 de este mes como consecuencia de una moción de censura, sobre la nueva estrategia de ciberseguridad.

Como vamos mal de tiempo, le agradezco su respuesta.

El señor **VICEPRESIDENTE:** Hemos superado con creces esa hora y cuarto que teníamos por compareciente, así que le pido, señora Quintana, que extreme la contestación en cuanto al tiempo, porque su primera intervención fue muy interesante pero muy abundante. Le pediría que redujera el tiempo, porque hemos pasado con creces el plazo y la hora que teníamos prevista. Gracias.

La señora **QUINTANA SERRANO** (Periodista experta en ciberseguridad): Muchas gracias.

Contestaré de forma telegráfica, porque muchas preguntas se han centrado en poner el acento en determinados aspectos de mi exposición. Aprovecharé la contestación para precisar aquellas cuestiones en las que no he podido extenderme y hacerlo detalladamente.

Se me preguntaba por el *hacking* ético y qué instrumentos legales están pendientes de desarrollar. Creo que he sido suficientemente explícita en todo lo que tiene que ver con filtraciones, o sea, hay que reformar el Código Penal en lo que tiene que ver con revelación de secretos y la responsabilidad que puede tener una persona que accede a sistemas informáticos, cuestión que ahora mismo puede estar incluso en el ámbito del terrorismo, porque los delitos informáticos en algunos aspectos se encuentran en el ámbito del terrorismo; y también la Ley de Enjuiciamiento Criminal en todo lo que supone que la Fiscalía pueda acusar por revelación de secretos cuando la información que se revela es de interés público, bien, como usted mencionaba, porque es un caso de *hacking* ético y la vulnerabilidad de un sistema o de una red, o bien porque es una información relevante de interés general. Por tanto, la sintonía estaría también con las recomendaciones del Parlamento Europeo en todo lo que tiene que ver con regular los alertadores o *whistleblowing* y filtraciones, y serían los puntos que he expuesto en mi comparecencia, que completarían la proposición de ley de protección del denunciante que ahora mismo se está tramitando y que deja fuera estos aspectos. Es decir, se podría aprovechar esa iniciativa legislativa para regular el *hacking* ético, las filtraciones y los denunciantes.

Acerca de otras realidades técnicas, como puede ser la responsabilidad en el Internet de las cosas, simplemente se trataría de ampliar la responsabilidad que ya se recoge en el real decreto del texto refundido de derechos de consumidores y usuarios, la responsabilidad de los prestadores de servicios por la seguridad de los productos y nuevas realidades tecnológicas en el Internet de las cosas. Sobre todo, hay que destacar la importancia de las filtraciones y los denunciantes, como muy bien su señoría llamaba la atención.

En cuanto al buenismo de los Estados, es cierto que la ciberguerra presenta muchas novedades —me he centrado mucho en explicar esto—, pero no es muy distinta de una guerra convencional, y en las guerras convencionales ha habido determinadas armas, como las nucleares, que, por su impacto humanitario, se han regulado, y se ha restringido su uso. Tenemos que ser conscientes de que, por mucho que sea etéreo, que sea un virus informático y líneas de código, el daño y el impacto pueden ser tan importantes como los de las armas tan lesivas que ya se han regulado, por no hablar de las armas autónomas, que no se controlan por los humanos. Por tanto, es cierto que puede parecer un planteamiento utópico, pero no es un planteamiento muy distinto a cuando ha habido otros retos en el ámbito bélico convencional y que la comunidad internacional ha sabido resolver. El principio sería una solución global, internacional bajo los criterios de quien dicta cuál es el marco de derechos fundamentales, que es Naciones Unidas.

Se me preguntaba por las campañas de desinformación y si no se ha demostrado. No voy a reiterar lo que ya han dicho otros comparecientes meses atrás, más cercanos en el tiempo al conflicto en concreto con el que se vinculaba este tipo de acciones. Reiteradamente el propio Centro Nacional de Inteligencia y su presidente, que, a pesar del cambio de Gobierno y en el departamento ministerial, sigue ostentando el cargo y ha insistido en ello en numerosos actos en los que ha intervenido, entienden que no está demostrado que en España se hayan producido campañas o guerra híbrida, como hay indicios de que en otros casos —sobre todo, donde está más documentado es en el de Estados Unidos— haya podido ocurrir. ¿Qué soluciones habría? Sucede como en el caso de cuál es la actuación de los Estados. Por

cve: DSCG-12-CM-102

suerte, el legislador español, como el legislador de todos los Estados, no tiene que inventar nada. Hay un marco, que son las recomendaciones de Naciones Unidas, que también en esto ha intervenido, y tenemos a los relatores de derechos humanos, que han establecido muy bien cuáles son las pautas y cómo hay que regular todo esto. Básicamente, por resumirlo, ninguna iniciativa que regule legislativamente la actuación de los agentes en la información, ni en los medios de comunicación ni de los agentes tecnológicos, y sí optar por campañas de formación a los usuarios y transparencia en la operatividad de estos agentes, que muestren cómo funcionan los algoritmos de los resultados de búsqueda o del muro de terminada red social. Por tanto, en cuanto al legislador español, mi petición y mi sugerencia sería que se mantuviese dentro del marco, porque la Comisión Europea en su informe sobre desinformación publicado hace unos meses, también con participación de expertos españoles y relatores de Naciones Unidas, ya ha establecido no regular, ya que inevitablemente incidiría en la libertad de información, y optar por medidas alternativas, como es la formación de los usuarios y la transparencia de todos los actores de la cadena informativa, también de los medios de comunicación.

El portavoz del Grupo Socialista me preguntaba por los ciudadanos y los Estados. Es cierto que la seguridad total no existe, y el Estado es vulnerable y los ciudadanos también. El daño es el mismo. La diapositiva que antes proyecté, que podría parecer un poco futurista, sobre las tres capas del ciberespacio, refleja un poco esto. No son compartimentos estancos. Por ejemplo, hay infraestructuras críticas en nuestro país que están operando con Windows, que ya no es seguro, y con otros sistemas operativos que ya no son seguros, y que son los mismos que los usuarios pueden estar utilizando, con la misma vulnerabilidad y la misma falta de seguridad. Por tanto, por decirlo rápidamente, no son compartimentos estancos y la vulnerabilidad de ambas esferas, la de los ciudadanos y la de los Estados, al final se contaminan, y hay que tratar ambas. No hay que dejar demasiada responsabilidad en los ciudadanos, más que en los Estados, y, sobre todo, hay que darles armas y formación para que puedan mantener la seguridad de sus comunicaciones y de su vida digital.

Efectivamente, la Directiva NIS, de seguridad en las redes, podrá ser una oportunidad cuando se trasponga al ordenamiento jurídico español para dar un marco jurídico global a todos estos retos que he intentaba resumir en las recomendaciones.

En todo caso, quedo a su disposición, porque me han planteado unas cuestiones muy interesantes, que telegráficamente no me da tiempo a responder.

Por acabar y no agotar el tiempo, el Grupo Parlamentario Popular me preguntaba por la competencia de los distintos organismos que ahora mismo tienen repartidas algún tipo de actividad y responsabilidad en el ámbito de la ciberseguridad de nuestro país. Sin duda, estas instituciones y los técnicos que trabajan en ellas son ejemplares, como el Incibe, en el ámbito de Industria, y el Centro Criptográfico Nacional, en el ámbito de la ciberseguridad y los ciberataques del Estado. A mi juicio, todas ellas están cumpliendo sus funciones. En el caso del Incibe, que digamos que es el interlocutor con los agentes y que muy bien se destaca en el primer grupo sobre el que me interpelaba, como pymes, pequeñas empresas, autónomos y ciudadanos, está siendo una buena herramienta para que accedan a información sobre dónde hay vulnerabilidades en tiempo real, incluso en caso de ciberataques concretos, como fue el caso de WannaCry, o incluso para poner a disposición de los distintos operadores, ciudadanos o empresas la vacuna para hacer frente a estos ataques. Por tanto, la competencia técnica de estos organismos está fuera de toda duda, al igual que la competencia de sus técnicos. Que la ciberestrategia es un buen instrumento para servir de paraguas, para que no haya distintas cabezas y estén bajo el mando del CNI resulta una buena solución. Pero aun así, creo que se pueden dar pasos, y al pedir más medios no hacía sino transmitir conversaciones privadas que he tenido con los distintos responsables de estos organismos, que, como es lógico, siempre piden más medios, al tiempo que hacerme eco de la declaración del representante del Grupo Popular, porque, aunque sí tenemos instrumentos para hacer frente a los ciberataques, las vulnerabilidades y las amenazas son tantas que nunca vamos a tener medios suficientes. Desde luego, no deberé decir que estamos en pañales, porque tenemos estos organismos, pero sí necesitaríamos muchos más medios para hacer frente a las amenazas a las que se enfrentan en su labor cotidiana.

El señor **VICEPRESIDENTE:** Muchísimas gracias a la compareciente, Yolanda Quintana, por su presencia e intervención, como a los otros comparecientes y a todos ustedes. Llevamos desde la una de la tarde.

Se levanta la sesión.

Eran las cinco y treinta minutos de la tarde.

cve: DSCG-12-CM-102