DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 82 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 13

celebrada el miércoles 28 de febrero de 2018 en el Palacio del Congreso de los Diputados

---

Página

---

cve: DSCG-12-CM-82

Se abre la sesión a las nueve y treinta y cinco minutos de la mañana.

COMPARECENCIAS:

— DEL SEÑOR MITXELENA RUIZ, SECURITY IBERIA LEAD EN ACCENTURE, 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 219/001044 y número de expediente del Senado 715/000356).

El señor **PRESIDENTE:** Señorías, buenos días.

Tenemos hoy una sesión relativamente cargada, con cuatro comparecencias, con lo cual apelo a su prudencia y a su continencia verbal.

En primer lugar, tiene la palabra el señor Mitxelena Ruiz, de Security Iberia Lead en Accenture, para informar sobre diversas cuestiones relativas a la ciberseguridad en España. El compareciente tiene la palabra por un tiempo aproximado de quince minutos.

El señor **MITXELENA RUIZ** (Security Iberia Lead en Accenture): Muy buenos días a todos. Estoy encantado de estar aquí. Creo que este es un buen foro en el que poder hablar un poco de la experiencia del sector. Cuando se me planteó compartir con vosotros el estado del arte de la seguridad, pensé hacia dónde podíamos enfocar la situación que tenemos, y he hecho la misma reflexión que hacemos a los clientes y las grandes compañías, por lo que voy a intentar acercar veinte años de experiencia a una situación actual, que creo que nos tiene que ocupar, más que preocupar.

¿Cuál es el escenario en el que movemos? Si miramos hacia atrás —gráfico para quienes nos gusta el cine—, probablemente este es un escenario que nos han venido contando los guionistas en los últimos años, es decir, ahora todo el mundo habla de infraestructuras críticas, todo el mundo hablamos de identidad digital, de la *deep web,* de las redes sociales, pero realmente el mundo del cine ya nos había anticipado algo que ahora está en nuestras vidas y en nuestro día a día. Por tanto, creo que debemos tener claro que ya no tenemos que apelar a si esto es un riesgo o no, sino que es un riesgo real. Las noticias, los medios de comunicación nos lo cuentan todos los días. Y estamos duplicando el número de incidentes cada año. Y estamos teniendo diferentes tipos de incidentes. Se están robando tarjetas, se están robando identidades, se están robando los nuevos elementos, como las *bitcoins* o criptomonedas. La red es un escenario en el que se mueve lo bueno y lo malo, y creo que hemos hecho el camino inverso: probablemente, hemos construido las infraestructuras sin pensar de verdad el modelo de gestión que debíamos llevar con ellas. Y esto no afecta solo al ámbito económico sino al político, y debemos tener en cuenta que hay dos tipos de agujero, de vulnerabilidad: la tecnológica y la humana, y creo que estamos jugando con ambas. Vamos a hacer un pequeño recorrido sobre ese escenario.

WannaCry es un antes y un después —no sé cuándo empezó esta Comisión, si fue antes o después de este programa—, creo que ha supuesto sobre todo un modelo de concienciación. WannaCry no es el mayor ataque que se ha dado directamente en las redes pero sí ha sido el más mediático, por lo que nos ha ayudado sobre todo a entender que estamos cambiando el mundo y que no nos hemos dado cuenta de que el mundo no está siendo gobernado, es decir, desde el punto de vista físico nosotros tenemos una serie de límites, territorios, leyes y elementos que en el ciberespacio no están definidos y los vamos a tener que definir. Pero es curioso que se da WannaCry y, como todos somos voluntaristas y todos tenemos la capacidad de ayudar, en un momento determinado nos damos cuenta de que en los años 2011, 2012, 2013 se había dado siempre el mayor incidente de los entornos de las redes. Y la curiosidad adicional es que el día que se produce el incidente en particular hay veinte, treinta, cincuenta, cien empresas que levantan la mano y dicen que acaban de detectar ese problema que está afectando directamente a todos, y eso sin estar coordinados, de forma absolutamente aleatoria y con un resultado que creo que fue muy limitante desde el punto de vista de las expectativas que teníamos en el sector de la ciberseguridad. Si a ello unimos las capacidades que tenemos en el entorno público, resulta que tenemos tres centros, cuatro y que cada uno nos va informando de una manera paralela de su visión sobre cuál es el estado de riesgo. Entonces, creo que en este aspecto lo que nos falta es intentar organizar y ordenar lo que tenemos entre manos. Tenemos que pensar que el cibercrimen, en todo su exponente, tanto en el ámbito económico, como en el terrorista, etcétera, innova, es decir, ya tenemos un modelo de innovación. Desde que empezó el mundo de las redes, desde que comenzaron los primeros virus se está innovando continuamente. ¿En qué? En poder llegar a aquella información, a aquel dato que para uno es interesante o crítico, lo que supone que la sociedad civil

cve: DSCG-12-CM-82

tiene que anteponerse a ellos y tenemos que pensar que desde la innovación vamos a tener que mitigar muchos de los riesgos que sufrimos.

¿A quién afecta los riesgos? Cuando empezó esto a finales de los años noventa y primeros del 2000, a las entidades financieras, que eran las que más estaban invirtiendo en estos elementos y las que más sonaban, pero desde hace ya unos cuantos años las entidades públicas que nos informan, Incibe, CNPIC y demás, ya nos están diciendo que afectan a todos los sectores y a todas las infraestructuras que pueden dar servicio a la sociedad, lo cual quiere decir que ya llevamos años viendo que llega, y todavía considero, personalmente, por conceptos de crisis y otros, que no hemos abordado directamente el problema desde la raíz.

¿A qué nos enfrentamos en la sociedad de hoy? Somos un país que quiere ser competitivo y que sabe que el mundo está cambiando, que estamos en un entorno global y que desde las directrices tiene que afrontar los cambios de la industria, de la sociedad, de la competitividad que hemos de tener en nuestro entorno y del modelo de gobernanza. Creo que desde hace dos o tres años todos hablamos de industria 4.0, de la transformación digital, de cómo van a cambiar mis negocios —por ejemplo, si estoy dedicando un negocio a un elemento productivo que mañana va a ser un servicio—, estamos integrando y comunicando el cien por cien de los elementos que estamos fabricando, como Eliotec, algo que genera la curiosidad, el lado infantil que tenemos todos a la hora de ver las tecnologías como un elemento de diversión, es decir, estamos abriendo un mundo pero no estamos gestionando de verdad los riesgos que estamos generando. Afortunadamente —y creo que este es un tema en el que estamos implicados—, Europa ha puesto en marcha desde hace dos años aproximadamente un conjunto de iniciativas y medidas en el que a través de las cPPP está integrando las capacidades públicas y privadas en definir las infraestructuras que debemos tener y cómo las debemos proteger, en innovar en aquel tipo de tecnología que sea europea y capaz de dar servicio a estos elementos y en gestionar gobernando con los modelos de gestión de incidentes y de prevención de los mismos. A partir de mayo —parece que se va a acabar el mundo, pero en el ámbito IT recuerdo el año 2000, cuando había que cambiar todas las aplicaciones porque se iba a parar todo tipo de negocio—, a partir del 25 de mayo, cuando entra en vigor la nueva Ley de Protección de Datos, cambian las responsabilidades, y las responsabilidades ya no están en el lado técnico sino en los consejos de administración. Esto es lo que está haciendo cambiar la visión de que la seguridad no es un coste sino un activo que tienen las organizaciones que te hace ser diferenciador. Las sociedades seguras se diferencian de las inseguras. Las empresas que trabajan desde el concepto de seguridad se diferencian de las que no trabajan en ese ámbito. ¿Y cuánto cuesta esto? Los estudios que se están haciendo dicen que el coste de la ciberinseguridad será en el año 2021 de seis trillones de dólares, que es dos veces el PIB de España o un poquito más, y no somos conscientes de que no estamos invirtiendo lo suficiente como para poder mitigar todos esos problemas. Además, estamos integrando en esa transformación digital nuestras infraestructuras críticas: la sanidad, el gas, el petróleo, la electricidad, es decir, estamos comunicados de forma permanente y tenemos los mismos riesgos en el ámbito del PC que en el ámbito de los entornos de gestión de las energías. ¿Qué más está pasando? Esto ya nos afecta a todos. Ya no afecta solo a la organización grande, ya no afecta solo a una empresa pequeña, afecta al ciudadano y afecta a toda la escala social. Por tanto, hay que trabajar en ese ámbito.

Dando por hecho que el mundo de la ciberinseguridad ha venido para quedarse, lo que tenemos que hacer es trabajar en construir un modelo que en el medio plazo nos permita prevenir cualquier tipo de riesgo. Elemento fundamental: faltan profesionales en el ámbito de la ciberseguridad. Faltan profesionales en otros ámbitos TIC pero este es uno de los elementos críticos, del que venimos hablando en los últimos cinco años y sobre el que todavía no hemos sido capaces de dar un paso firme para construir un concepto de futuro. ¿Cómo estamos en España? Estamos en un cambio global, estamos en un cambio de modelo social, diría que estamos construyendo el futuro desde el error, porque la clave es construir, no esperar a que construyan otros. Creo que debemos tener visión, hace falta visión, cultura y liderazgo, y creo que este es el foro que debe liderar el futuro del país. Hay que centrarse en el ciudadano, en nuestro empleado, en nuestro cliente, nos tenemos que centrar en ellos. Hay que ayudar a nuestras industrias a que sean competitivas en el entorno global, es decir, ya no estamos compitiendo de forma local y en un entorno físico sino en un ecosistema muy diferente que nos hace cambiar los modelos de negocio. Y una cosa que está pasando en la transformación de las empresas es que esto no significa informatizar lo que ya hacía antes, sino cambiar la forma de pensar y la forma de hacer, y probablemente la forma de gobernar, en un escenario absolutamente nuevo y del que no tenemos claro dónde están las fronteras.

cve: DSCG-12-CM-82

¿Qué suele ser lo ideal? Que alguien nos traiga la máquina del saber, metamos directamente las ideas y tengamos un resultado. Desafortunadamente, eso no se da, por lo que tenemos que confiar en los modelos profesionales, tenemos que saber colaborar con ellos. Queremos construir sociedades digitales, *smart cities,* que sean más cómodas, en favor del usuario, reduciendo el consumo de energía, etcétera, y todo ello tiene por detrás un modelo tecnológico y un modelo de gestión que tenemos que poner en marcha. Además, en un mundo digital siempre hay una incertidumbre: quién está al otro lado del ordenador, quién está al otro lado del teléfono. Es decir, está cambiando de verdad la forma de hacer y ser y este es otro de los retos que debemos tener todos, el de definir un modelo de identidad digital, que hoy está muy lejos de lo que se requiere. En esta incertidumbre pasa lo que ocurre siempre, que el factor humano está dentro de las redes e, igual que las empresas aprovechan el mundo digital para ese cambio, sucede en el lado de los malos. Lo vamos a llamar cibercrimen desde el punto de vista económico, podemos hablar también del terrorismo, en definitiva podemos hablar de todo el concepto del mal, que ya está en las redes, ya se ha transformado, más rápidamente que nosotros, y va por delante. Así que nos tenemos que poner las pilas, entre comillas, y dar pasos conjuntos para pode evitar eso. Es decir, tenemos que saber con quién hablo, con quién estoy, con quién hago negocios, quién está de verdad en el ámbito de las redes. Hay que llegar al concepto de identidad digital.

Visión personal —y me tenéis que disculpar, porque esto es algo que se dice a las empresas de este país y creo que hay que compartir—: hemos vivido muchos años de bonanza, hemos vivido muy bien, creo que hemos ido en el tractor y nos ha ido bien. Hemos pensado que estábamos compitiendo directamente con otros tractores, con lo cual hemos sido un país competitivo. Pero, desafortunadamente, en este cambio digital de Internet ha venido otro tipo de vehículo, otro tipo de empresas, que se llaman Google, Facebook, Apple, etcétera, que tienen nuestros datos, que están creando su modelo y que nos condicionan en nuestra forma de ser y de hacer. Y creo que es un tema que debemos tener absolutamente en consideración. ¿A qué nos lleva esto? A que si seguimos en el modelo tractor nos van a ir pasando siempre en esa carretera. Llegaremos al objetivo pero tarde, dejaremos de ser un entorno competitivo y una sociedad cien por cien liberal. Otro de los grandes problemas que tenemos es que cuando nos damos cuenta del problema automáticamente aparecen cientos de champiñones, cada uno repitiendo: ¡yo sé cómo hacerlo!, y terminamos atascados, preguntándonos cuál es el objetivo, cuál es la ruta, hacia dónde vamos y cuál es el camino que debemos trazar. Viéndolo en un símil de dibujos animados, se parece un poco a la carrera de los autos locos, en la que unos van por el aire, otros por el mar, pero no hay de verdad un modelo que nos pueda incluir a todos y nos pueda permitir construir un futuro sensible y seguro.

En ciento cincuenta años hemos visto un cambio absoluto, hemos vivido cuatro revoluciones: la del vapor, cuando aquí empieza el tren, después la electricidad, el petróleo y ahora estamos en el dato. Creo que el dato es la clave de los nuevos negocios, de la nueva sociedad y, sobre todo, de los entornos de seguridad. ¿Cómo podemos ayudar a esta sociedad que estamos construyendo a ser más eficiente y a ser más confiable? Durante el siglo XX hemos transformado las compañías, haciéndolas más modernas; digamos que hemos innovado. Ahora hay que cambiar directamente el tema, y siempre nos hemos encontrado con que el futuro y el presente están ligados a personas, procesos, productos y tecnologías. Entonces, creo que hoy el ámbito más tangible de cualquier compañía u organización es la información. Por tanto, la clave de todo lo que estamos construyendo se llama dato. Las empresas están pensando en qué hacer con tantos datos y cómo pueden cambiar de verdad el futuro. Se está intentando cambiar los modelos de organización y hacer que la gente de sistemas empiece a pensar en negocio, y, con esos datos y una serie de herramientas matemáticas, poder predecir el futuro, con sus ventajas y desventajas. Hemos construido Internet, seguimos teniendo procesos, personas y tecnología y hemos abierto la puerta a la transformación digital del mal, con los riesgos y aquello que nos puede afectar directamente en nuestra vida diaria.

¿Dónde estamos? En la seguridad percibida. Creo que en la sociedad civil siempre hay una seguridad percibida, por la que el individuo se siente más cómodo, y creo que en Internet debemos llegar también a la seguridad percibida. La que tenemos hoy es relativa. Los que trabajamos en el ámbito de la seguridad sabemos que el riesgo es alto. Los que estamos trabajando con tecnología probablemente no estamos pensando en ello, hacemos un punto y parte y nos centramos exclusivamente en lo que estamos haciendo, pero creo que hay que empezar a concienciar desde edades tempranas en el buen uso de la tecnología, hay que empezar a concienciarse de la importancia de la información que manejamos, de nuestra organización, de nuestro negocio, y creo que esa es la clave de ponérselo difícil al ámbito del mal. ¿Dónde estamos hoy? En un entorno global, en un ecosistema nuevo. Nos ha impactado la crisis y creo que ese

cve: DSCG-12-CM-82

ha sido un tema global que nos ha hecho cambiar. No es una crisis de la que nos vamos a recuperar sino desde la que tenemos que cambiar, y además en un mundo global. Estamos trabajando en el ámbito europeo y realmente los marcos regulatorios están afectando a todos los sectores: el financiero, de energías, etcétera. Estos marcos regulatorios nos están obligando a hacer lo que probablemente no hemos hecho con anterioridad. Debemos gestionar el riesgo en referencia a nuestros ciudadanos y nuestras empresas, y eso es algo que está por construir. Posiblemente estamos todavía en la versión 1.0 y nos tenemos que basar en la tecnología, en la innovación, en la innovación propia y en nuestras personas. Y creo que la clave es la confianza. En el ámbito del ciberespacio nos tenemos que preguntar si hay fronteras —esta es una de las grandes preguntas—, si somos un país digital, si existe una España digital, si realmente hay delimitaciones, un concepto IP, un concepto sobre comunicación, un concepto de altura. Este es uno de los grandes elementos que tenemos.

¿Cómo podemos regular o cómo podemos legislar los conceptos del ciberespacio, que es otro tema en el que nos debemos alinear con el resto? Claramente, hemos generado un nuevo mundo, que tiene un montón de ventajas pero que también tiene un montón de incertidumbre. La gobernanza es clave y creo que es el Gobierno el que tiene que poner, de verdad, las pautas y las claves acerca de dónde estamos, adónde vamos y con quién. Creo que Europa juega un papel fundamental. ¿Qué es lo que tenemos que defender? ¿Estamos defendiendo información, estamos defendiendo ciudadanos, estamos defendiendo las infraestructuras críticas, estamos defendiendo nuestro futuro? Creo que este es otro de los elementos. ¿De quién? ¿Quién nos ataca? ¿Quién es el enemigo? ¿Es alguien que me quiere robar? ¿Es un país? ¿Es un elemento distorsionador? Creo que tenemos un escenario complejo, del que no va a ser fácil salir de forma limpia y hacia delante. Entonces, hay que aprender a defenderse y a prevenir, dos conceptos.

Hablaremos dos minutos sobre ciberinteligencia, porque sé que no hay mucho tiempo. En cuanto a los primeros pasos, ¿qué plan de acción llevaría yo? Educación desde primaria, es decir, hay que enseñar, igual que hacen otros países, como Reino Unido o Francia, que llevan ya cinco, seis años educando en la ciberseguridad y en el buen uso de la tecnología a los menores. La clave es que todos veamos el riesgo desde la educación. Igual que tenemos la educación vial, que está en nuestros planes de estudios, la educación cibernética es clave en este asunto. Y además la generación de profesionales desde la formación profesional hasta el entorno universitario. Nosotros hemos trabajado en conceptos de formación profesional dual y ya están saliendo los nuevos profesionales de FP en ciberseguridad. Pero este tiene que ser un tema global, no voluntarioso, solo de algunas empresas y entidades.

Debemos definir nuestro escenario, el modelo de gobernanza, la seguridad, legislar, que sé que no es fácil. Probablemente ya se habla de ciberderecho. Igual hay que cambiar también la forma de ver el espacio y los elementos, pero creo que debemos definir los de gobernanza. Y un tema que ya está encima de la mesa es la certificación, la certificación de las personas, de las empresas, de los productos. Igual que tenemos teléfonos y otros medios de comunicación que tienen cierto tipo de certificaciones en el ámbito ignífugo, eléctrico y demás, se va a tener que certificar en ciberseguridad y vamos a tener que trabajar con esas herramientas. ¿Por qué? Porque la seguridad es igual que la calidad, es una parte del proceso. Y si definimos desde el principio las cosas con garantía será bastante más difícil que nos ataquen en un momento determinado. Entonces, en cuanto al plan de acción, si nos referimos al ámbito público y los foros en que nos movemos, todo el mundo somos sabios y todos hemos hecho ciberseguridad. Pero realmente creo que hemos hecho el 1.0, con más voluntad que estrategia, y hay que pasar al 2.0, que ha de estar gestionado desde arriba. ¿Y en qué nos tenemos que basar en esta transformación? En la gobernanza, tenemos que definir los modelos de gobernanza. No podemos competir entre instrumentos públicos y privados, tenemos que colaborar y tenemos que definir quién manda, quién lidera. Creo que esa es una clave. También educar, atraer el talento. Este es un país que tiene muchísimo talento en el ámbito de la seguridad y las tecnologías. Lo malo es que se nos ha ido fuera una cantidad importante. ¿Cómo somos capaces de generar más talento y de atraer nuevamente al que ha salido fuera? También hay que innovar, tener centros de competencia exclusivos de seguridad en los diferentes sectores: sanidad, turismo, etcétera. No podemos hacer las cosas solo genéricamente, también tenemos que actuar sobre los elementos claves del futuro del país. Y además considerar la obligación que tenemos desde el punto de vista de país de dar seguridad a nuestros ciudadanos y a nuestras compañías. Vamos a pensar que tenemos muchas compañías digitales y muchos ciudadanos virtuales. ¿Cómo hacemos para ir transformando el mundo físico a este global? Si vamos a Google y buscamos ciberseguridad, nos aparecen millones de documentos que hablan de ello, millones de incidentes que han sucedido. Generalmente, la ciberseguridad es un elemento dirigido a la reacción, igual que el control de calidad. Por

cve: DSCG-12-CM-82

tanto, hay que llevar la seguridad a los conceptos sobre diseño. Si vamos a ciberinteligencia, aparecen muchos menos. Pero si vamos a Wikipedia, aparece el Cispa, que es un acuerdo que tiene el Gobierno americano con sus empresas privadas para intercambio de información en caso de riesgo global, es decir, colaboración público-privada. Esta web no habla de un tema genérico sino de un país que ha generado un modelo de colaboración, que entiendo que tiene éxito para ellos porque al final están gobernando a su manera una parte importante del ciberespacio.

Pero también nos enfrentamos a más cosas, es decir, nos enfrentamos a temas que están latentes, como el espionaje, ya sea político, industrial, económico, etcétera. En mi experiencia profesional, hemos visto muchos casos de empresas críticas en las que el enemigo estaba dentro con muchos meses de antelación y cuando nos hemos dado cuenta ha sido tarde. Por tanto, creo que todos debemos trabajar en pos de que eso no se dé. ¿Qué hacen? Nos copian, nos siguen, nos vigilan, nos ganan en los concursos por un euro. Es algo que sucede en la realidad y las redes han abierto la posibilidad de llegar más fácilmente a los entornos de la información. Estamos en la época de la posverdad, estamos en una época complicada. Cualquier cosa que se dice, a la velocidad que vamos, nos la creemos. Nos mandan un wasap y lo reenviamos directamente, sin chequear previamente quién lo envía, qué dice o qué no dice. Somos todos responsables —y digo todos— de que esto no ocurra. Es decir, creo que debemos aprender a saber manejar correctamente las tecnologías y saber filtrar aquella información que llega. Es la desinformación, es decir, se está jugando en la red a cambiar conceptos, a cambiar el mundo. Hay gente que está interesada por intereses a, b o c en cambiar directamente el rumbo de la historia. Entonces, son cuestiones sobre las que ir dando pasos. Pero, como dice Thomas Frey, que es un hombre del DaVinci Institute, el futuro se construye hoy, es decir, no hay que esperar a que llegue, nosotros tenemos que construir el futuro. Uno de los elementos claves que ha de tener un país si de verdad quiere ser un país de futuro y competitivo es generar los modelos de formación en ciberseguridad y ciberinteligencia. Necesitamos profesionales, necesitamos compañías, necesitamos músculo en un ámbito que va a ser clave en el devenir de nuestros tiempos.

Mi primera conclusión es que estamos en construcción, no nos alarmemos. Probablemente tengamos que hacer un plan de transformación. La segunda conclusión es sobre qué haría yo, algo que contamos en todos los foros. La expresión inicial es colaboración público-privada, que ya ha empezado. Posiblemente tengamos que quitar personas del camino, aquellas no entiendan que este no es un tema personal sino colectivo. Hay que ser generosos. La palabra generosidad debemos ponerla todos en nuestro frente. A continuación, I+D+i, apostar por nuestras empresas, por la compra pública innovadora. En un *think tank* del año 2007 alguien de un ministerio me dijo que cada vez que sacaban un concurso llegaban tres americanos y dos británicos con un producto, mientras que las empresas españolas iban con una idea. Le contesté que los americanos hacían lo mismo hace diez años: sacaban las ideas, generaban productos, los financiaban y los promocionaban. Entonces, hay que cambiar. Creo que en este país hay que estar contentos de los que triunfan y no hay que tener ese sentimiento de envidia si alguien de casa lo ha hecho bien. De los fracasos creo que se aprende y de los éxitos tenemos que vivir de forma efímera. Además, nos tenemos que alinear con Europa y hay que tener un modelo estratégico; en este ámbito Europa juega un rol fundamental. También hay que definir un modelo de gobernanza, que ya se está definiendo en Europa, la Ley NIS. Y educación digital, la clave del futuro es educación digital. Y otras preguntas que no sé si son para este foro o si las vamos a tratar después: ¿Qué es lo que tenemos que ir protegiendo? ¿Quién es el enemigo? ¿Quién lidera esto, quién es el líder? Nos hacen falta líderes, alguien que diga que manda esta persona, este estamento, este entorno. ¿Cómo nos coordinamos? Está muy bien que nos juntemos, que digamos que vamos a luchar juntos, que vamos a trabajar juntos, pero hay que saber coordinarse y hay que saber gestionar correctamente un entorno como este. ¿Qué debemos compartir desde el ámbito de la información? En los métodos más adecuados, ¿confidencialidad? ¿Dónde hay que trabajar? ¿Quién filtra y analiza la información? Antes hemos hablado de la posverdad, la desinformación, las *fake news,* ¿quién tiene que filtrar eso? No es sencillo, porque es un tema que conlleva una visión también relativa. ¿Quién paga esto, quién paga esta fiesta, quién financia? El gran problema que tenemos en este ámbito es que nos hemos olvidado de la importancia que tiene la ciberseguridad, y el plan de financiación que tenemos en este país y en Europa, en general, está muy lejos de los requisitos que deberíamos tener. Algunas veces ya lo he dicho: si desde el año 2001 hubiese habido alguna fragata menos, algún tanque menos, si hubiéramos invertido directamente en este ámbito, probablemente tendríamos un sector líder en la Unión Europea. No se ha hecho por otros motivos supongo, pero creo que todavía estamos a tiempo de cambiar algunos elementos. Finalmente, ¿cómo trabajamos todo esto y

cve: DSCG-12-CM-82

cómo hacemos que sea democrático? La gran dificultad está en democratizar algo que está abierto y que, al final, debe tener unas pautas, unos modelos y unas reglas. Y no queda más que seguir adelante, es decir, no se trata de que veamos el escenario blanco, negro o azul; estamos en un escenario en el que tenemos que trabajar juntos y construir, y tenemos que empezar con todo esto.

Muchas gracias. Las preguntas que tengáis y pueda responder, con mucho gusto; y las que no deba responder, igual. Creo que este es un entorno abierto.

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

Si dedicamos menos a fragatas y corbetas me temo que acabemos navegando a vela o a remo. Pero, en fin, esa es una observación marginal.

Tiene la palabra en primer lugar por el Grupo Vasco el señor Legarda.

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

Muchas gracias al compareciente también, por las ilustrativas explicaciones que nos ha dado. Ha sido una intervención muy rápida y muy a borbotones. Es un poco precipitado que intervenga, pero alguna cuestión le plantearé.

Una de las últimas cuestiones o preguntas que se ha hecho es quién es el enemigo, yo supongo que será un enemigo poliédrico. Quizás el concepto del enemigo lo autogeneremos nosotros mismos, como un cáncer. Yo creo que el problema con el que nos enfrentamos ya está constatado. Tenemos una gran capacidad de producir cambios, pero una lenta capacidad de asimilarlos, que es una característica del ser humano. Cuando aceleramos mucho somos capaces de generar cambios e innovar, pero estamos viendo que tenemos muchas dificultades socialmente como humanos en asimilar esos cambios. Yo creo que es lo que está pasando en este momento. El pretender pensar las consecuencias, y luego hacer el producto, va contra la lógica del ser humano; eso nunca pasa porque lo vemos en bioética. Entonces lo que nos está pasando es consustancial también a nosotros mismos. Así pues, a la pregunta ¿quién es el enemigo? Yo contesto: depende.

En realidad el gran problema de la ciberseguridad es que es un producto de una manifestación global y, sin embargo, las gobernanzas no son globales sino locales. ¿Qué problema tenemos? Pues que normalmente en nuestros ámbitos locales afrontábamos esto desde nuestros modelos de gobernanza, cuyo paradigma es la democracia. Por ello, tenemos una gran dificultad para afrontar la gobernanza de estas situaciones porque son globales y no tenemos una gobernanza global, y mucho menos que responda a criterios democráticos. Esta es una de las crisis de la construcción europea, no digo nada de una construcción global. De momento, más allá —es mi opinión y le pregunto si usted la comparte— de empezar desde abajo, desde lo micro, e ir sensibilizando y protegiéndonos desde lo individual hacia lo colectivo —lo individual somos nosotros en el uso de las tecnologías—, así como enseñar a las personas que nos rodean, sobre todo a los más jóvenes, de los riesgos que se corren en el mundo que nos vamos metiendo, deberíamos ir subiendo en escala, pero estamos topados. Es fácil de hablar, pero no veo una gobernanza global que pueda gestionar una realidad que es ecuménica, como la globalización, las tecnologías y las empresas.

Le pregunto si quizás haya que construir, pero no invocando la solución final. Tiene que haber una gobernanza global, pero no la vamos a conseguir a corto plazo. Por eso, debemos irnos protegiendo desde lo pequeño, haciendo un discurso desde lo pequeño hacia lo grande. Empezar el discurso diciendo que tenemos que afrontar esto y que es posible ponernos al mismo nivel que el riesgo, no lo veo viable. Hay que ser más posibilistas y afrontarlo con un poco más de melancolía o realismo y trabajar desde lo muy concreto, ya veremos más tarde cómo podemos ir subiendo en la escalera. No veo viable esos grandes conceptos de gobernanza global, aunque hay avances muy importantes en la Unión, en concreto en la protección de datos que precisamente estaremos tratando estos próximos días. Eso es lo preventivo; luego está lo reactivo con todas las agencias, las empresas. Desde mi punto de vista habría que lanzar un mensaje mucho más realista y mucho más cauto. No sé si usted comparte esta percepción general.

Muchas gracias.

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

Por el Grupo Parlamentario Ciudadanos, tiene la palabra el señor Salvador.

cve: DSCG-12-CM-82

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

En primer lugar quiero felicitar al compareciente, por una parte, por la completísima presentación que ha hecho, porque no solo ha expuesto su opinión sino que ha contado su experiencia y ha trasladado precisamente ya buena parte de las respuestas a preguntas que se pudieran suscitar, y por otra, porque ha dejado el marco muy bien definido y con un contenido absolutamente trabajado. Yo comentaba con el ponente hace un momento algo que dije en una intervención hace algún tiempo para intentar sensibilizar al conjunto de la Cámara y también al conjunto de la sociedad española. Cuando hablamos de ciberseguridad —usted ha dado como ejemplo las películas que anticipaban ya la era en la que nos íbamos a mover— parece que es una cosa de frikis, de gente que maneja los ordenadores, que es un juego de buenos y malos. De hecho si alguien es muy malo lo fichamos con los buenos, y si gana el videojuego o la videopartida al malo, entonces estamos triunfando. Sin embargo, estamos hablando de un cambio de era que apareja muchísimas transformaciones. En cierta ocasión puse el ejemplo de la calzada romana o de las rutas marítimas para que el conjunto de la Comisión viera que ha habido momentos de cambio y de transformación muy importantes en la humanidad, al igual que ahora lo está siendo Internet, con todas las posibilidades que nos ofrece la tecnología y también la innovación.

¿Dónde están las diferencias? Pues que antes resolver el problema de seguridad en la calzada romana por muy grande que fuera era un poco más fácil, porque protegías a las gentes que se desplazaban. Lo mismo ocurría en la navegación, y lo sabemos por las cartas marítimas, porque había barcos que reforzaban esa seguridad. El problema que hay desde mi punto de vista es que el marco regulatorio y los instrumentos de respuesta ante las amenazas y los riesgos son lentos, porque en este momento estamos hablando de cómo nos ponemos de acuerdo en identificar quién es el enemigo. Se ha dicho que todavía no tenemos identificado quién es el enemigo, pero yo entiendo que el enemigo es la inseguridad. A partir de ahí lo que hace falta es acabar con esa inseguridad, es decir, si nos dotamos de seguridad venceremos a ese enemigo que es la inseguridad. Además, los cambios son muy rápidos porque precisamente Internet, la tecnología y la innovación, permite que las amenazas y los riesgos evolucionen permanentemente y de esta forma toda la gente que está en ese tema —que es muy dispar, tal como ha comentado en su intervención— va evolucionado también y va encontrando el hueco en el sistema por el que poder penetrar.

Por otra parte, el marco regulatorio y la Administración reaccionan despacio. Entendemos que es fundamental la colaboración público privada, porque la empresa no se puede permitir la inseguridad en ningún momento y tiene que actuar también reactivamente. El tema es cómo coordinamos a ese sector privado, con sus aportaciones, con la garantía de que el marco es el mismo que estaría gestionando la propia Administración y que lo haga coordinadamente con ella. Cuando usted decía quién tiene que marcar el liderazgo y quién tiene que marcar la toma de decisiones, yo entiendo que esto tiene que hacerlo la Administración, es decir, la gobernanza tiene que venir desde la vía de la representación institucional y política, porque si dependiera entonces de la empresa privada estaríamos en otro tipo de intereses a la hora de poder gestionar eso. El tema está en que la Administración no es capaz de garantizar por sí misma esa seguridad y, por tanto, tiene que apoyarse en un sector privado porque también le afecta este tema y por eso es fundamental.

Compartimos plenamente lo que ha dicho sobre la educación. Si la seguridad no empieza a combatirse con los hábitos de cada uno de nosotros, sabiendo que estamos depositando nuestra vida entera dentro de un móvil o en la nube o en cualquier otro sitio, estaríamos bastante mal. Por tanto, entendemos que eso es absolutamente acertado, como toda su intervención.

Me ha preocupado bastante cuando usted ha dicho que el coste de inseguridad en 2021 se puede evaluar en 6 trillones de dólares. El tema es: ¿estamos siendo capaces de actuar sobre una amenaza tan grande como esta? Usted ha dicho que se están multiplicando los ataques, que se están multiplicando las pérdidas. La sociedad está concienciada, hoy existe una Comisión como esta. ¿Cree que en el año 2030 tendremos nuestras herramientas de defensa perfectamente organizadas de manera que seamos capaces de evitar estos costes de la inseguridad? Digo esto porque si hay costes por inseguridad son producto de que no estamos protegidos y están muchas cosas en riesgo. Una cosa es que haya pérdidas económicas, pero también ha añadido infraestructuras críticas. Por tanto, no estamos hablando ya simplemente de si alguien puede llevarse el dinero de alguien, o si alguien se puede llevar las ideas de alguien pirateándolas; estamos hablando de cómo le pueden cambiar la vida a un persona metiéndole en un móvil contenido que no sea suyo, copiando el contenido de otra persona. Antes a una persona le ponían un poquito de droga en una maleta y después le detenían diciéndole que llevaba droga, pero ahora pueden meter cosas que

cve: DSCG-12-CM-82

no sean adecuadas en un móvil y detenerle diciendo que eso estaba dentro del móvil. Eso puede pasar hoy también perfectamente porque la tecnología lo permite.

Para terminar, quiero volver a felicitarle por toda la intervención que ha hecho, aunque he de decir que el apostolado es también el camino para tratar de concienciar a todo el mundo. Yo quisiera preguntarle, desde su experiencia, y viendo las reacciones de una Administración que es lenta y de una clase política que cambia cada cuatro años y suele tener una visión cortoplacista en un tema, si cree que vamos en la buena dirección o en el bueno camino, si piensa que estamos empezando a sincronizar los relojes de todos los actores que formamos parte de la defensa contra esa inseguridad, o si por el contrario prevé que podamos tener turbulencias y un descontrol muy importante en el futuro. Al contrario de lo que ha dicho un compareciente —a quien yo respeto mucho— sobre que la gobernanza es local —entiendo lo local por los hábitos de los ciudadanos y las empresas—, yo creo que la gobernanza en un momento como este es absolutamente global.

Muchas gracias.

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

Para que no caigamos en confusión cuando el señor Mitxelena ha hablado de trillones se refiere a trillones en sentido americano, a *trillions;* es decir, en nuestro continente serían billones, no trillones.

El señor **SALVADOR GARCÍA:** Luego ha dicho 700 millones en 2015.

El señor **PRESIDENTE:** Cuando dice trillones está pensando en…

El señor **MITXELENA RUIZ** (Security Iberia Lead en Accenture): … dos veces el PIB nacional. Ahí yo creo que ya me habéis entendido, son billones.

El señor **PRESIDENTE:** Un poco menos.

Gracias, señor Salvador.

A continuación, por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, tiene la palabra el señor Mayoral.

El señor **MAYORAL PERALES:** Buenos días.

Quiero agradecer al compareciente su exposición. Yo creo que lo interesante de una exposición, al contrario de lo que suele decirse habitualmente, no es encontrar la respuesta sino poner bien las preguntas, porque eso nos va a permitir reflexionar en esta Comisión hacia dónde ir. Hay algunas cuestiones que se han planteado finalmente que me parece que son claves. ¿Qué protegemos? Esa es una de las cuestiones clave que hay que responder. Desde nuestro grupo creemos que hay que proteger el ordenamiento jurídico, hay que proteger la democracia y los derechos humanos, como un elemento central. A partir de ahí, vamos a ver cuáles son los bienes jurídicos protegidos que se despliegan a través de esa finalidad, que debe tener un ordenamiento democrático, y cuáles van a ser las herramientas democráticas de las que nos vamos a dotar.

¿Quién es el enemigo? A mí me parece que es bueno separar la paja del trigo, es bueno separar las cosas que son distintas, o por lo menos distinguirlas, porque si no lo hacemos así corremos serios riesgos. No es lo mismo una red de *hackers* que se dedica a hacer *phishing* y a robar en cuentas bancarias, que un grupo terrorista que ataca a una estructura estratégica del país a través de sistemas informáticos y que puede incluso pretender extorsionar al Estado, o que haya gente que opine cosas que al Estado no le gustan en las redes sociales. Son tres cosas distintas. Desgraciadamente en los debates que hemos tenido en esta Comisión ha habido la estrategia del gazpacho, que ha sido la de mezclarlo todo como si todo fuera igual.

Eso hila en buena medida con otra pregunta que planteaba el compareciente, que me parece muy interesante: ¿quién lidera este asunto? Este asunto puede ser liderado obviamente por los Estados, y en concreto por los Gobiernos democráticos elegidos por la ciudadanía, o este viaje puede ser liderado por las grandes corporaciones, que en esta materia pueden llegar a tener más poder que la mayoría de los Estados en el mundo. Podemos poner algunos nombres, pero creo que en la cabeza de todos está quiénes pueden ser los actores que deciden, cuando ponemos una palabra, qué es lo que vamos a buscar, o los que hacen que aparezcan unas cosas u otras cuando estamos en las redes sociales. A mí me gustaría que nos hablase, si puede, sobre ese asunto. Se ha establecido un debate en las intervenciones anteriores entre las gobernanzas locales y esas gobernanzas globales, pero parece ser

cve: DSCG-12-CM-82

que las gobernanzas globales tienen mucho más que ver con las grandes corporaciones, que con los organismos internacionales constituidos por los Estados para poder afrontar los retos del futuro. Ese tema creo que es un reto para la democracia porque cuando el futuro de la humanidad se decide en un consejo de administración, en función del capital que tienes en una empresa, y no en función de los votos que tienes en unas elecciones, la democracia está en peligro.

Hay otro asunto muy interesante, me refiero a cómo puede afectar toda esta cuestión de la seguridad en el tráfico, por las tres diferenciaciones que hacía al principio: los que atacan el tráfico jurídico simplemente para asaltar caminos —lo que ha sido robar de toda la vida, pero en este caso con otras herramientas—; los que realizan actividades en contra de infraestructuras críticas; y los que lo hacen para difundir unas ideas, unas veces equivocadas otras menos equivocadas, o incluso equivocadas a cosa hecha. Ahí hay un problema que tiene su origen en la libertad de imprenta. La libertad de imprenta ha permitido desde el siglo XIX que las personas puedan decir lo que estimen oportuno y siempre ha existido desde el poder político la tentación de reducir la capacidad de las personas para poder ejercer la libertad de información y la libertad de expresión como un elemento básico para la existencia de un ordenamiento democrático. En ese sentido, me gustaría que nos dijera cómo piensa que puede afectar, por una parte, el debate de las *fake news,* y por otra, el debate de la versión oficial. Estamos en un momento en el que se está planteando la vuelta a la versión oficial.

Hay formaciones políticas que creen que debe haber organismos gubernamentales que pongan el sello de la versión oficial. Cómo cree que afecta eso a un elemento básico en la democracia como es la libertad de información, porque si hay versión oficial no hay libertad de información. Sería muy interesante conocer su opinión, máxime en un Estado como el nuestro donde el Consejo de Informativos de Televisión Española acusa directamente al Gobierno de manipular la información a favor de sus intereses. ¿Qué riesgos existen de la generación de órganos estatales que controlen la información que libremente se pueda dar en la red y cómo afecta eso a la seguridad? La seguridad implica el ejercicio de la libertad, la seguridad de poder ejercer la libertad de expresión en un momento en el que se encuentra seriamente amenazada, incluso en su vertiente artística como hemos podido ver recientemente en la Feria de ARCO, donde ya ni el arte está privado de la posibilidad de expresarse libremente en un Estado como el nuestro.

Muchas gracias.

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

A continuación, por el Grupo Parlamentario Socialista, tiene la palabra el senador Álvarez Villazán.

El señor **ÁLVAREZ VILLAZÁN:** Muchas gracias, señor presidente.

Señor Mitxelena, en primer lugar, quiero darle las gracias por su intervención, que ha sido suficientemente clara y pedagógica, porque nos ha dado la visión que tiene un profesional como usted sobre este grave problema, por el que creo que estamos todos preocupados. Usted seguramente tendrá más conocimiento que nosotros sobre este asunto. No voy a pretender ni mucho menos decirle lo que debe hacer, porque creo que está aquí para informarnos como experto de lo que realmente piensa. Me voy a limitar a señalar, siguiendo su intervención y algunas notas que tenía tomadas de otras declaraciones de otros expertos en ciberseguridad, las posibles dudas que creo que me podría resolver.

En principio, añadiendo el dato que usted daba de perjuicios que se podían crear, tenía otro dato ya que hace poco he leído que en 2021 podíamos estar hablando de más de 6000 millones de dólares de pérdidas originadas por los ataques a todos los sistemas críticos.

El señor **PRESIDENTE:** Eran 6 millones de millones.

El señor **ÁLVAREZ VILLAZÁN:** ¿No eran 6000 millones?

El señor **PRESIDENTE:** Eran 6 millones de millones.

El señor **ÁLVAREZ VILLAZÁN:** Pues corrijo mis datos, porque eran datos que había sacado del Foro Económico Mundial. Es un dato increíble y creo que es suficiente como para estar preocupados.

Me parece muy interesante lo que ha dicho sobre la necesidad de que España y Europa desarrollen una industria potente en ciberseguridad. Creo haberle entendido decir que hay un importante riesgo si no lo hacemos así, ya que podríamos estar adquiriendo productos que no fabricamos nosotros sobre ciberseguridad, con lo cual estaríamos siempre dependiendo de otras naciones. En este sentido, y teniendo en cuenta que la mayoría de los ataques provienen de otros Estados, entiendo que señala esto

cve: DSCG-12-CM-82

como un riesgo. Me gustaría preguntarle cómo ve este proceso de poder crear una industria propia, si lo ve usted factible, si realmente se han dado pasos avanzados en este sentido y si ese modelo de colaboración, que he creído entender que usted propone entre entes públicos y privados, ha comenzado en España, así como si existe ya alguna experiencia positiva, quizás a través de empresas como Telefónica. Quizás no le haya entendido muy bien, pero creo que ha dicho que en la Unión Europea ya se creó una experiencia en este sentido. Quería preguntarle si realmente esto ha funcionado, si hay resultados tangibles de este esfuerzo hecho a nivel europeo.

Otro problema que ha señalado es la falta de personal especializado, en este sentido me parece muy interesante la propuesta que ha hecho. Me gustaría que concretara un poco más, si puede, sobre el dedicar una importancia fundamental a la educación. Ha señalado dos aspectos, no solamente educación en la universidad sino también la educación en la enseñanza media; es decir, ha propuesto empezar desde los primeros años a introducir en nuestros escolares ese concepto de riesgo que podemos tener en estos momentos.

En otras de sus declaraciones de hace tiempo hablaba de la necesidad de unas certificaciones de ciberseguridad en las empresas, similares también al certificado de calidad. Ahí quería preguntarle: ¿se ha avanzado algo en este sentido o todavía es una idea que se ha lanzado pero no se está realmente cumpliendo?

Asimismo, usted ha señalado el interés de llevar la ciberseguridad en todas las empresas solicitando una inversión continúa. Me parece un tema muy interesante. Querría preguntarle qué dificultades hay para que las empresas entren en este concepto y estén dedicando más recursos para el tema de la ciberseguridad.

Teniendo en cuenta que el nivel del riesgo —del que se habla en distintas informaciones— que tiene España de sufrir un ciberataque es muy alto, no sé si conoce la Estrategia de Seguridad Nacional de 2017. ¿Cree que los objetivos que se plantean en ella son realmente los adecuados para estos momentos? Entiendo que en la Estrategia de Seguridad Nacional de 2017 se definen muy bien las amenazas y los desafíos, estableciendo una graduación de cuáles pueden ser los peligros. Desde mi punto de vista, creo que están muy bien diseñados, pero a la hora de señalar los objetivos nos encontramos con que son muy ambiguos porque se habla de desarrollar un modelo integral de gestión de crisis, o promover la cultura de la seguridad nacional, lo cual me lleva a pensar que realmente estamos en pañales, que estamos prácticamente iniciando un proceso que quizás debería estar, dado los riesgos de los que estamos hablando, mucho más avanzado y que se debería estar destinando más esfuerzos a esta tarea.

Por último, me gustaría hacerle una pregunta más concreta centrándome en Telefónica, teniendo en cuenta que puede ser la empresa puntera en nuestro país. ¿Cree que tiene también esa falta de personal especializado? ¿Cree que la colaboración de Telefónica con la Administración General del Estado es la suficiente para afrontar este problema? ¿Qué opina de la infraestructura que tenemos en nuestro país para prevenir estos ataques? En este momento si una empresa sufre un ataque esta se lo comunica al Gobierno. Después el Gobierno es quien actúa a través del Consejo Nacional de Seguridad que depende del Centro Nacional de Inteligencia, del cual depende el Consejo Nacional de Ciberseguridad, del cual depende también a su vez el Centro Criptológico. El Ministerio de Defensa actúa por su cuenta, el Ministerio del Interior con el Ministerio de Industria también actúan por la suya. A pesar de la labor muy buena que creo que está haciendo el Incibe y de que la colaboración, según datos de los que disponemos, entre la Policía y la Guardia Civil está siendo bastante coordinada y positiva, me gustaría preguntarle si no cree que sería necesario unificar todos estos organismos para conseguir una mayor operatividad de los mismos.

Creo que no se me olvida nada más. De nuevo, muchas gracias, por su intervención.

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

Quizás el tema del certificado de seguridad pudiese formar parte de las conclusiones de esta ponencia, pero eso lo decidirán ustedes.

Para terminar esta primera ronda tiene la palabra, por el Grupo Popular, la señora Vázquez.

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

Quiero dar las gracias al señor compareciente, al señor Mitxelena Ruiz. Ha sido sin lugar a dudas una comparecencia muy didáctica en la que hemos tomado notas de las diferentes consideraciones y aportaciones que usted nos ha hecho en el día de hoy.

cve: DSCG-12-CM-82

Cuando preparaba su comparecencia he encontrado, tirando de hemeroteca, que hablaba en 2003 de un ataque masivo a la red. En aquel momento ya usted hablaba de concienciación, de que en esos momentos era hackear páginas para hacer una identidad falsa, pero que eso podía ir a más. Después en 2016 llegó a hablar de *hackerpocalypsis,* es decir, un apocalipsis cibernético que pudiera existir. Sin lugar a dudas es usted un avanzado ante lo que nos esperaba en España y en el mundo. Por otra parte, la concienciación es fundamental. Usted lo anunciaba en 2003 y nosotros consideramos que las empresas y la sociedad en general tienen que concienciarse del riesgo que tiene el ciberespacio, que es algo muy bueno pero que también tiene sus riesgos y hay que saber defender y prevenir.

Nosotros planteamos hacer esta Comisión antes del ciberataque masivo que sufrimos en España en el mes de abril, creo recordar. Nosotros ya habíamos hablado aquí de poner en marcha esta ponencia, considerábamos que era un reto para la Comisión de Seguridad Nacional hablar de seguridad y traer aquí los expertos, entre los que se encuentra usted.

Tomo nota de algo que me pareció muy oportuno, cuando hacía el símil con la educación vial que era la educación digital, la educación cibernética. Nosotros fracasamos en ese tema, no tenemos esa educación ya en primaria para los niños, creo que debemos tomar nota de cara a esas conclusiones finales, señor presidente.

El modelo de identidad digital es un problema. Hablamos mucho de la identidad digital, que es muy fácil atacar en las redes sin tener una identidad digital y hacer intromisiones sin saber quién es el que está del otro lado. Es lo que se llama la incertidumbre digital. Nosotros consideramos que de alguna manera se debe poner freno a este asunto. Esto es un desafío, quien quiera jugar en el ciberespacio debe identificarse y jugar con todas las credenciales.

Le voy a hacer una serie de preguntas que he preparado como obligación, como país nosotros debemos de darle seguridad a nuestros ciudadanos y a nuestras empresas. Ese es el pilar fundamental de esta ponencia. Conclusiones que podamos remitir al Gobierno, a las empresas, para que nuestras empresas y nuestros particulares se sientan más seguros, por eso le voy a hacer una serie de preguntas.

Con respecto a la gobernanza, que ya ha hablado el compañero de Ciudadanos, en materia de protección de ciberespacio ¿considera adecuadas las actuales estructuras de participación, tanto de la sociedad civil como del sector privado? ¿Considera que los actuales planes de estudio —esta la tenía preparada sin saber que usted ya iba a responder, pero la formulo igual— tanto en los niveles preuniversitarios como en los universitarios se encuentran adaptados? Como puede ver, no caía en la educación primaria. Hablaba de universitarios y preuniversitarios, no se me pasaba por la cabeza cuando ayer preparaba estas preguntas que otros países como Francia y Reino Unido ya tenían desde primaria una educación cibernética. ¿Disponemos de recursos y talentos suficientes para participar de forma activa en las políticas públicas de I+D+i que pudieran impulsarse desde el propio Gobierno? ¿Cree que los recursos asignados a la protección del dominio del ciberespacio son suficientes y, sobre todo, se encuentran bien orientados en pos de la eficacia, que no eficiencia, de los mismos? ¿Considera que los canales de colaboración público-privados están generando las suficientes sinergias como para hacer eclosionar un tejido productivo fuerte e innovador en esta materia? En estos días, en el Congreso de móviles hablábamos del 5G. El Gobierno aprobó 20 millones de euros para un plan piloto del 5G. Se están haciendo cosas, pero ¿es necesario intensificar esa colaboración público-privada? De lo que se habló aquí: ¿Quiénes considera que son los actores que pueden constituir una amenaza para nuestro Estado y contra la sociedad en su conjunto? ¿Qué medidas de protección del ciberespacio considera que deberían tomarse en consideración a la hora de promover la participación de la sociedad en la ciberdefensa? Con un apunte que usted hizo de que faltan profesionales en el mundo de la ciberdefensa, ¿cree que una reserva estratégica de talento en materia de ciberdefensa y de ciberseguridad, lo que denominamos desde el Grupo Parlamentario Popular la ciberreserva, constituiría una herramienta apropiada a la hora de promover esa participación de la sociedad civil y ayudar o paliar así a la falta de profesionales que pueda tener en estos momentos en España? Me quedo con una frase que usted apuntó ahí: el futuro crea el presente y nosotros estamos aquí para recibir las aportaciones que usted como profesional de la materia nos haga y hacerlas llegar a las conclusiones de la ponencia.

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

Tiene la palabra el señor compareciente para responder. ¿Le parece bien diez minutos?

El señor **MITXELENA RUIZ** (Security Iberia Lead en Accenture): Voy a intentar resumir, porque creo que habéis hecho algunas preguntas comunes. Voy a ir por orden. Señor Legarda, estamos de acuerdo.

cve: DSCG-12-CM-82

El gran problema es que la velocidad del cambio siempre está encima de la asimilación de riesgo que tenemos y me parece un tema absolutamente natural. El gran concepto que tenemos que manejar es que no hay que pensar lo que pasará, y si un día pasa tendremos que asumir los resultados, sino que hay que construir con el objetivo fundamental de que no pase. Llevo veinte años en este mundo de ciberseguridad, veinticinco en Internet, he visto cambiar muchas cosas, he visto transformar muchas cosas, he apostado siempre por un concepto que se llama la educación. Cuando en su día fundamos nuestra compañía ese 21 que, en el norte, lo primero que hicimos fue formar al sector. La primera ocupación era generar cultura. Desafortunadamente en mi vida laboral siempre he ido antes de tiempo, yo empecé en calidad cuando no se hablaba de calidad y al cabo de veinticinco años la calidad está en los procesos. Cuando empezábamos nosotros en esta materia nos recibían muy bien, nos escuchaban muy bien, pero nunca nos contrataban. Hasta que llegaba el cliente final —un hecho diría yo— al que le decía si no cumples una serie de procesos probablemente no seas mi proveedor en el futuro. Entonces empezó a cambiar todo esto. Somos un mundo reactivo, es decir, la velocidad de cambio es tan grande que al final imponer las medidas es un concepto reactivo. Pero estoy de acuerdo. Que el enemigo es el hombre en sí mismo. No hemos cambiado tanto en los últimos siglos desde el punto de vista del comportamiento humano, lo que ha cambiado son los medios y el acceso a esos medios. En la distancia física, los riesgos eran relativos, en la distancia virtual estamos todos en el mismo escenario. La clave es la educación. La clave es formar desde lo que son con los estadios primarios a toda la sociedad del futuro. Entender muy bien lo que es el buen uso de la tecnología en ese concepto de lo que tiene que hacer una sociedad democrática y justa y, a partir de ahí, construir. No vale solo que digamos que ya sabemos que pasarán las cosas, sino que tenemos que construir un modelo que haga más difícil que eso se produzca. Si se produce probablemente no sea en el lugar en el que tenemos que manejar nuestros derechos y nuestras obligaciones.

En el concepto gobernanza nos debemos a nuestra sociedad, simplemente expongo una realidad que es la complejidad que tiene gobernar de verdad en el ciberespacio. Existe un poder legislativo, existe un poder Judicial, existe un poder político que lo tenemos establecido con unos territorios, unas limitaciones y una serie de elementos. En el ciberespacio esto es absolutamente abstracto y es algo en lo que creo que también tenemos que trabajar. La parte judicial, la parte del derecho, es la que tiene que empujar también a entender muy bien si es que existe un modelo de gobernanza local, si es que existe un modelo de gobernanza transversal o si no existe gobernanza porque es absolutamente inviable llegar a alguna conclusión. No sé si te he respondido.

Señor Salvador, hemos comentado antes lo que es la evolución del tiempo y lo que son los conceptos de riesgo. Creo que los enemigos somos la propia sociedad. Cuando estás trabajando en el ámbito industrial mi mayor enemigo es China. ¿Por qué? Porque se fabrica más barato y porque compite con otras herramientas. ¿Qué hemos hecho muchas veces? Ir a fabricar a China. Algunos han tenido resultados positivos y otros negativos. Estamos aprendiendo en el cambio cuál es el modelo de empresa y cuál es el modelo de entorno en el que tenemos que trabajar. Cuando yo empecé en calidad a finales de los años ochenta, la verdad es que veía la calidad muy lejos de lo que eran los procesos y veía siempre el control de calidad. Me metía en acerías y en industria y veía pieza a pieza el calibre, medir las dimensiones, medir la calidad del producto y demás. Veinticinco o treinta años después la calidad es un proceso que está embebido. ¿A qué ha ayudado eso? A que existe una normativa de certificación. A que cuando existen las licitaciones se exigen que se cumplan con una serie de parámetros, a que cuando estoy trabajando con clientes o proveedores estoy trabajando en un modelo de calidad concertada. Mi sueño, ya han pasado veinte años, con lo cual esto es complejo, es que llegue un día en el que aquí estemos trabajando en un modelo de seguridad concertada. Si fuera en el año 2030, ojalá. Los ciclos aquí son más complejos sobre todo por su dimensión. La dimensión de la cadena de valor en una empresa es limitada, la dimensión de la cadena de valor que tenemos en Internet es absolutamente ilimitada. Si vamos construyendo, por lo menos en nuestro entorno, un modelo que nos exija y que nos permita trabajar con aquellas entidades o personas que nos den unos modelos de garantía, estaremos construyendo el modelo del futuro. Ojalá en el 2030 digamos que estamos preparados contra estos ataques. ¿A quién ataca el malo? A quien es más fácil de atacar hoy. O tengo un objetivo claro y tengo que trabajar con una serie de elementos y estrategias o trabajo directamente en un modelo automatizado y el que es más débil es el que sufre de forma directa la amenaza y el impacto. Un elemento que no hemos hablado. Una cosa es la amenaza y otra cosa es el impacto de la amenaza. Cuando hablamos de infraestructuras críticas, la misma amenaza que tiene un puesto de trabajo es la que puede tener directamente una central térmica. El impacto es diferente si me quedo sin información, así directamente influyo en un entorno que puede ser

cve: DSCG-12-CM-82

crítico en la sociedad. Hay que seguir evangelizando. Empecé en calidad evangelizando, en 1994 evangelizando. No soy cura, no tengo complejos de eso, pero he estado también en el ámbito ciber evangelizando. Me considero un emprendedor. No soy un experto en seguridad. Soy una persona que intenta desarrollar los negocios y los equipos y aportar valor a las empresas y a la sociedad. Ojalá en el año 2030 nos podamos volver a ver, si no es en este foro, en otro, y podamos decir que hemos avanzado lo suficiente como para estar satisfechos de los pasos que hemos dado. No sé si había alguna pregunta más.

Señor Mayoral, que me quiere poner en un aprieto, pero yo voy a contestar desde mi visión personal como lo estoy haciendo en todo momento. Hablamos del ordenamiento jurídico de lo que es la democracia. Estamos cambiando el mundo, es un mundo complejo. Aplicar las leyes actuales al mundo de Internet no es el elemento directo. Lo que tenemos que cambiar es entender lo que es el ciberespacio, aplicar los modelos de libertad. Soy partidario de poner límites al concepto de libertad. ¿Dónde está el límite? La libertad de expresión es algo que tenemos todos, pero hay que poner rayas a lo que es la libertad. La interpretación es un elemento relativo en el que no te puedo ayudar. Los que estáis en el ámbito político tenéis diferentes visiones a la hora de analizar lo mismo, con lo cual para mí no es fácil poder situarme sobre eso. Pero sí entiendo que Internet nos ha dado un modelo democrático en lo bueno y en lo malo. En lo malo tenemos que intentar poner algún tipo de barreras o límites que nos permita jugar en las mismas condiciones. Cuando yo empecé en Internet los primeros foros que montaban, los primeros *chats,* que eran en el entorno del fútbol, la gente se insultaba permanentemente. Era un lugar, año 1995 o 1996, en el que el *chat* del club de fútbol cuyo objetivo fundamental era insultarse entre la gente. Al final qué hacía el club, cerrar el *chat*. En un elemento que es absolutamente diferente, que tiene un mundo multimedia, está bien que podamos opinar, está bien que existan diferentes opiniones pero no soy capaz de medir el grado de limitación que debe tener cada una de las opiniones. Este es un tema que queda mucho más en vuestro ámbito.

La diferencia entre lo que es *hacker* físico y demás, estamos cambiando de rol. Cuando antes alguien te robaba un banco ibas físicamente a la sucursal y tenías unas cámaras y unos elementos que te podían monitorizar y tenías incluso la seguridad física. Cuando estás en la red en el mismo escenario tenemos a los *hackers,* a los pederastas, a los enemigos públicos número uno, tenemos a los inquisidores, a los terroristas, realmente tenemos todos el mismo escenario y no sabemos donde estamos. No sabemos físicamente dónde está cada uno. La tecnología nos permite además jugar al engaño. Puedo estar utilizando tu ordenador y hacer cosas que tú no estás haciendo pero alguien piense que eres tú. Ha sido otro de los elementos que ha introducido el señor Salvador. ¿Se puede utilizar el mundo de Internet para cambiar ciertos elementos para ver que alguien ha hecho lo que no ha hecho? Se hace, no se puede. ¿Se puede chequear que alguien lo ha hecho? La ventaja de Internet desde el punto de vista de las evidencias es que se puede dar la trazabilidad adecuada siempre que no seas un gran experto. Estamos construyendo un mundo. Me parece complicado. No es lo mismo que tengas gente que esté haciendo *phising* y te robe credenciales. Eso es un tipo de riesgo. No es lo mismo que tengas a los grupos terroristas trabajando en Internet, haciendo captación de personal. No es lo mismo y hay que gestionarlo de forma diferente probablemente. Cuando estamos en la ordenación civil habitual tenemos interior, tenemos defensa, tenemos otros elementos. En la red, habrá conceptos que serán de interior y otros de defensa. ¿Cómo vamos a cambiar esto? Creo que este es otro de los trabajos que tenemos que hacer. Es otro de los elementos a hacer. Un tema importante que ha dicho es quién lidera y tenemos que tener claro ¿quién está liderando Internet? Las multinacionales, os he expuesto claramente que han llegado, se han impuesto, nos están condicionando y nos están gobernando. Ellos han creado su escenario, ¿Por qué? Porque como en el ciberespacio, como he dicho antes no existe gobernanza, pero existen países que están haciendo lo mismo. No voy a dar nombres, pero puedo dar tres o cuatro países que están construyendo su modelo de gobernanza. Algunos utilizan a las empresas porque están en su *pool* a la hora de manejar información y otros lo hacen con sus equipos y sus infraestructuras. ¿Quién debe liderar? Estamos en el mismo escenario, ¿cómo se debe construir el quinto espacio y cómo se debe gobernar? Y hay que hacerlo democrático, porque si no será un fracaso de todos y tendremos un futuro bastante incierto. Creo que te he contestado a todo.

Sobre las *fake news* o no *fake news,* lo que decía antes, es un criterio de opinión, un criterio de manejo. Aquello que es mentira es mentira y eso hay que tenerlo claro. Aquello que es opinión hay que dejarlo en ese concepto. Que las opiniones de uno vayan en contra de las opiniones de otro no quiere decir que sean falsas. Interpretar todo eso debe ser un tema de democracia desde el punto de vista de

cve: DSCG-12-CM-82

cómo se gestiona. Gestionar cualquier tipo de información de quito, pongo, censuro o no, es un elemento de riesgo de algo que hoy está abierto y, como antes decía, algunas cosas deberían ser censurables, desde el punto de vista de la ética, pero hay otras que son diferentes opiniones que en mi modesta opinión debería ser abierto, pero no daría más vueltas a eso. No sé si te he contestado a todo.

Señor Álvarez, me has hecho un interrogatorio perfecto, pero creo que algunas de las cosas las hemos contestado. ¿Dónde está el riesgo de la industria? Eso es otro de los grandes desconocidos que tenemos. Siempre se ha dicho desde que empecé en este mundo que había un conjunto de países que nos escuchaban. Desde Internet tenían las comunicaciones interceptadas y tenían la capacidad teórica de llegar a cierto tipo de escuchas. Internet es un mundo abierto en el que vale todo, en el que la tecnología está por encima de cualquier pensamiento que tengamos. Se puede hacer todo con tecnología. Efectivamente, existen países que están negando a ciertas tecnologías de terceros por la falta de certeza pero por la sensación de que puede ser una puerta abierta a entrar en la información propia. Apostar por tecnología propia en seguridad es un tema de confianza. Apostar por generar una industria propia es algo en lo que vamos con retraso. Antes comentaba el *think tank* del año 2007, la parte pública entendía en ese momento que no teníamos las herramientas, las estructuras ni las personas como para poder construir un sector. Esto con las diferentes iniciativas que se han dado está cambiando. Con Incibe, poco a poco se van generando algunas líneas de dinamización de lo que tiene que ser el mundo del desarrollo de esta industria, pero la clave se llama Europa. Es decir, Europa es quien ha generado una CPPP, que es un tema de colaboración público-privada que se hace entre ECSO, European Cyber Security Organisation, que es una organización que nos aúna a todo el sector privado y al de educación y al de innovación conjuntamente con la Comisión Europea. Se ha dotado de un conjunto de fondos. Se cerró la firma en el año 2016, se han cerrado con los diferentes grupos de trabajo durante 2017. Empezamos a tener proyectos en los que vamos a trabajar y espero que los primeros resultados empiecen a estar en el año 2020. Ahí se está trabajando en la certificación, que es otro de los elementos que hemos comentado que es clave. Si miramos hacia casa existen diferentes entes y estamentos que están intentando sacar su sello de certificación, el CCN-CERT, la asociación de presos de ciberseguridad, cada uno está generando su modelo de negocio, no sé si esta es la palabra clave, el CCN en base al esquema nacional de seguridad. Europa también estaba trabajando directamente en estos entornos de certificación de las personas y las empresas y lo que se está haciendo es intentar definir un estándar para las personas, un estándar para los conceptos de empresa que nos sirva de base en este entorno de futuro. El futuro será que cuando tengamos las licitaciones públicas exigiremos que las empresas cumplan una serie de parámetros: medioambiente, calidad y seguridad, y que los profesionales que trabajen en datos críticos que estén manejando estén certificados en los niveles adecuados de este entorno.

Más cosas. Amenazas, desafíos e impactos. Eso ya lo hemos hablado. La amenaza es común y el impacto depende muchas veces de dónde está la infraestructura. Nos tenemos que tomar en serio lo que son los conceptos de infraestructura crítica. Muchas cosas nos han contado. En los foros que he estado a nivel internacional he visto ataques reales desde el año 1999 al 2000 a infraestructuras de agua, a infraestructuras de electricidad en otros países, en el ámbito terrorista, y otros elementos que no se han hecho público, pero que desde los entornos de inteligencia y seguridad nacional saben que se están produciendo. Sabéis que todos los años las infraestructuras críticas reciben un conjunto de incidentes. Es verdad que se ha hecho un esfuerzo relevante desde que se creó el Cnpic en el año 2007, cuando no había recursos, pero poco a poco se le ha ido dando peso. Diez años después las infraestructuras críticas de este país, sobre todo las grandes organizaciones, están trabajando en aras de proteger en las mejores condiciones, desde el punto de vista físico lógico, aquello que nos tiene que dar servicio en nuestro día a día. Aquí tenemos un *gap*. No podemos proteger el 100 % de las organizaciones y de las infraestructuras. Ahí hay también un papel relevante en las comunidades autónomas. Cuando hablamos del sector financiero estamos, entre comillas, protegiendo como un elemento crítico a los tres grandes, pero hay más entidades financieras que dan servicio y soporte en el entorno del país. Ahí es donde las comunidades autónomas deben apostar y deben apoyar en un modelo organizado la defensa propia de este tipo de infraestructuras.

Respecto al país y a las organizaciones que tenemos. También se ha comentado. Estamos un poco desorganizados desde el punto de vista que tenemos demasiados instrumentos y estamentos que hablan de lo mismo: Dirección de Seguridad Nacional, Mando único en Ciberdefensa, CCN-CERT, Incibe, Cnpic. Con la nueva ley *mix* europea que nos va a obligar en la gestión de crisis, lo que se está creando un elemento vertical, vamos a tener un interlocutor válido en las infraestructuras críticas, un interlocutor que

cve: DSCG-12-CM-82

sea válido en los conceptos ciudadano-pyme y creo que nos vamos a organizar mejor. Como antes he expuesto, nos hace falta una reflexión de transformación sobre todo de un plan a diez años vista. Más o menos he dado respuesta al señor Álvarez.

A doña Ana Vázquez, me has hecho un conjunto de preguntas interesantes, pero creo que alguna de ellas ya estaba contestada o al menos ya estaba planteada. La identidad digital, Internet solo será un elemento demográfico y será posiblemente gobernable cuando lleguemos de verdad a la identidad digital. Una persona, una conexión. No sé si seremos una IP, no sé si seremos un número de teléfono o una huella, pero cuando tengamos identidad digital podrá ser más fácil poder construir de verdad lo que tiene que ser un modelo de gobernanza democrática en el ámbito de Internet, en el ámbito del ciberespacio.

Había una serie de preguntas. La gobernanza, estábamos hablando de ello, creo que todavía nos falta definir liderazgo. ¿Quién lidera esto? ¿La Dirección de Seguridad Nacional? ¿La Comisión que estáis trabajando en este momento que va a definir cuál va a ser el modelo de gobernanza? Hace falta tener líderes. En otros países, cuando se ha establecido la relación público-privada se ha definido un líder, una cabeza. Esa cabeza es quien comunica, quien impulsa, quien gobierna y quien tiene los recursos. Hace falta tener de verdad una cabeza y no seis. En este momento tenemos un modelo voluntarista donde hay que ser generosos —siempre pongo la palabra generosidad delante— y alguien tiene que liderar y gobernar independientemente de su condición. De si vengo de Defensa, de si vengo de Presidencia, de si vengo de Interior. Es un elemento clave de cara sobre todo a la sociedad y a la colaboración de lo que tiene que ser el sector privado en este ámbito.

La educación, lo hemos dicho, si miráis el número de master que tenemos en España en Ciberseguridad hay como 85, todos diferentes, todos definidos desde el concepto de esto es un negocio más y no existe de verdad un modelo de definición de lo que tiene que ser el profesional de la ciberseguridad en sus diferentes aspectos. Siempre digo que en las empresas el profesional de seguridad tiene que ser alguien de negocio. En la parte de gobierno tiene que ser alguien de concepto país. Alguien que no sea político. En el concepto tradicional que sea un concepto país. Tenemos que mirar esto siempre a largo plazo independientemente de los ciclos que existan cada cuatro años. Esto es un concepto de futuro y de construcción de un país.

La parte primaria es una asignatura pendiente. Llevo muchos años hablando con Incibe, con el ministerio, en nuestra comunidad autónoma con la parte de Educación. Alguna comunidad autónoma está por delante de lo que es el Gobierno central, porque hay una mesa de educación que por unas circunstancias u otras tiene un ritmo más lento que el resto. Vamos muy tarde y creo que tenemos que poner de verdad foco en todos estos conceptos de formación. No solo hay que formar a los menores, hay que formar a los formadores. La forma de educar debe ser diferente cuando estamos llevando a los policías municipales, a los policías nacionales, a los ertzaintzas directamente a enseñar la educación vial, deberíamos pensar lo mismo. Quién debe de educar de verdad a los menores y los formadores que son quienes tienen que velar día a día por el buen uso de la tecnología.

En la universidad, se nos pasó Bolonia. En la época de Bolonia este país debía de haber impulsado la carrera de ciberseguridad. Han pasado diez años más y estamos en el momento de ponerlo en marcha. En la parte de formación profesional igual. El gran *gap* que tenemos en el ámbito de ciberseguridad nos exige que la formación no sean ciclos de seis años sino que sean ciclos cortos y que tengamos gente capacitada, más que formar hay que capacitar a los entornos profesionales. Cuando estamos hablando del entorno tecnológico entrenar, porque este es un tema de entrenamiento de alto rendimiento, no es un tema baladí, independientemente de las tecnologías que estamos implementando.

Disponemos de recursos en talento en I+D, disponemos de algunos recursos, de algún talento, pero tenemos que tener más recursos y atraer más talento. El talento ha huido de este ámbito, porque desafortunadamente los entornos de la crisis, el sector PIC, en general, y la ciberseguridad, en particular, se han infravalorado. Hemos tenido que sufrir siempre las penalizaciones de las mesas de compra, del coste. Esto es muy serio y la capacidad de la gente que trabaja en este ámbito se merece una tranquilidad. Tener gente que tiene un perfil alto trabajando con salarios de 1000 euros es inviable que sigan en el sector o en compañías en las que están trabajando. Ha emigrado talento a las grandes multinacionales. Una cosa buena que podemos decir que en grandes multinacionales como Google, Microsoft y demás, hay expertos de seguridad de este país, con los que he trabajado personalmente, por cierto, que están liderando la ciberseguridad. De ese escenario que decíamos de los grandes actores que están manejando en este momento el ciberespacio. Existe talento, pero hacen falta recursos. Si no es una fragata es un F-35, me da igual, pero existen costes en los que realmente… Algún elemento que digamos no existe

cve: DSCG-12-CM-82

dinero, existe dinero y creo que tenemos que cambiar por los modelos de inversión desde el punto de vista de lo que es construir el ámbito de ciberespacio donde realmente un avión muy poco tiene que hacer, en el espacio sí, en el ciberespacio no. ¿Quiénes son los enemigos? Hemos hablado de esto, no hay que dar muchas vueltas. Los canales de comunicación están mejorando. Desafortunadamente este es un mercado de muchas expectativas en el que hay demasiadas empresas pequeñas y poco músculo. Nos hace falta concentración de empresas que tengan la capacidad de dar un paso adelante.

No he contestado antes al tema de telefónica, porque tiene su sociedad particular, pero yo siempre he puesto una frase con ellos desde el año 2002 y 2003, si yo voy por la autopista y pago un peaje, lo que quiero es que no tenga baches. Si estoy comprando comunicaciones, lo que quiero es que sean seguras. Este es un poco el rol que deberían cumplir las grandes infraestructuras, si no, deberían de ser gratis. Tenemos que asumir que existían una serie de problemas.

Las medidas para poder participar en ciberdefensa, la clave en este país es que si nos tomamos en serio esto hay que tener más recursos, nos tenemos que alinear con los recursos de Europa. Muchas veces en la innovación hemos hecho un esfuerzo real en los cambios de transformación. Probablemente hemos tenido demasiado café para todos. Porque todo el mundo quería innovar, nos ha faltado hacer foco en los proyectos estratégicos. Creo que en ciberseguridad es absolutamente necesario porque en los tiempos que estamos hay que hacer foco en los proyectos estratégicos. Aprovechar Europa, que también tiene un conjunto de recursos a los que aportamos desde el país, porque existen un conjunto de proyectos tractores en los que deberíamos ser uno de los entornos líderes. En Europa se está jugando una batalla de liderazgo en la industria de ciberseguridad. Francia e Italia tienen muchísimo peso. Pero a nivel nacional, entre los centros tecnológicos y las empresas especializadas estamos haciendo un esfuerzo por tener proyectos que se lideren desde aquí y nos permitan construir también nuestra propia industria.

La última pregunta creo que era la de la reserva estratégica, esto está en el ámbito global. Nosotros tenemos que definir un modelo, hacer un acto voluntarista de trabajo conjunto, es un elemento puntual. En el modelo gobernanza de colaboración público-privada hay que integrar las estructuras público y privadas. No se trata de decir cuando haya un problema te llamo. Tenemos que trabajar de una forma coordinada. Tenemos que decidir qué tipo de perfiles nos hacen falta para esto. Nos hace falta siempre el *hacker*, el elemento técnico, hace falta juristas, hace falta expertos, hace falta estrategas, hace falta definir el modelo y luego crear ese entorno de trabajo conjunto donde las empresas se deben de ver compensadas. Es decir, las empresas están formando en talento, están desarrollando talento, están dando servicio a sus clientes. No podemos quitar los recursos de las empresas en un momento determinado sin que estén cumpliendo también con sus obligaciones. Creo que entra todo dentro de un marco global en el que la palabra reservista se ha interpretado mal en el ámbito del entorno. Ya se ha hablado que si esto es el ejército Pancho Villa y cosas de estas. No es el espíritu supongo. El elemento clave es que esto es un concepto público-privado. Todos nos jugamos el futuro. Tenemos que saber trabajar de una forma ordenada y con los recursos adecuados. No sé si me dejo algo.

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

Tenemos acordado que habrá un segundo turno. Quiero advertir a sus señorías, que llevamos un cuarto de hora de retraso en este momento y que tenemos ya al siguiente compareciente en la sala. Sin embargo, voy a abrir el segundo turno, empezando por el señor Legarda.

El señor **LEGARDA URIARTE:** Muchas gracias, señor presidente. No voy a intervenir.

El señor **PRESIDENTE:** Gracias.

Tiene la palabra el señor Gutiérrez.

El señor **GUTIÉRREZ VIVAS:** Solo quiero dar las gracias al compareciente.

El señor **PRESIDENTE:** Muchas gracias.

Tiene la palabra el señor Mayoral.

El señor **MAYORAL PERALES:** Intervengo para aclarar que no tenía ninguna intención de ponerle en un brete. Simplemente me interesaba mucho conocer su opinión, sobre todo, porque creo que a veces existe un fetiche de las nuevas tecnologías y hay conductas que están contempladas en el ordenamiento jurídico, se puedan hacer con elementos materiales o con elementos virtuales. A veces queremos inventar el agua tibia, pero está inventada hace mucho tiempo. Los límites de la libertad de expresión y del derecho

cve: DSCG-12-CM-82

a la intimidad y a la propia imagen están contemplados en el ordenamiento jurídico. Esas limitaciones existen, pero se quiere ir a más, lo que se está planteando es ir a más, es ir al control de medios de comunicación y a poner sellos de versión oficial. Eso se hace en el mismo Estado en el que los trabajadores y las trabajadoras de la información de los medios públicos están denunciando que desde el Gobierno se utilizan los medios de comunicación a favor de sus intereses y en contra del resto de las fuerzas políticas, violentando el pluralismo político en nuestro país y manipulando la información. Cuando ese mismo Gobierno que es acusado de realizar esas prácticas está intentando implementar una estrategia para la construcción de una versión oficial, nos encontramos con una amenaza a la libertad de información.

Ese era el objeto de la pregunta anterior y la conceptualización de aquello de las *fake news*. Y no hay peores *fake news* que las del señor Marjaliza en el caso Púnica.

Gracias.

El señor **PRESIDENTE:** Nadie ha dudado de la inocencia de su intervención, señor Mayoral.

Tiene la palabra el senador Álvarez Villazán.

El señor **ÁLVAREZ VILLAZÁN:** Simplemente quiero dar las gracias al compareciente por su intervención.

El señor **PRESIDENTE:** Tiene la palabra la señora Vázquez.

La señora **VÁZQUEZ BLANCO:** No voy a intervenir. Muchas gracias.

El señor **PRESIDENTE:** Señor Mixelena, ¿quiere hacer alguna observación sobre la libertad de información?

El señor **MIXELENA RUIZ** (Security Iberia Lead en Accenture): Simplemente quiero dar las gracias al señor Mayoral. No ha sido ponerme en un brete, creo que estabas hablando de cosas que van más allá de lo que yo debo exponer. Soy un amante de la libertad y, a partir de ahí, sobre esos otros elementos, que son las consideraciones que vosotros podéis poner encima de la mesa, no me toca opinar en este momento.

El señor **PRESIDENTE:** Muchas gracias. Eskerrik asko.

— DEL SEÑOR SÁNCHEZ ALMEIDA, DIRECTOR JURÍDICO Y MIEMBRO DE LA JUNTA DIRECTIVA DE LA PLATAFORMA EN DEFENSA DE LA LIBERTAD DE INFORMACIÓN (PDLI), PARA QUE EVALÚE LOS DERECHOS A LA LIBERTAD DE EXPRESIÓN Y DE ACCESO A LA INFORMACIÓN, ASÍ COMO LOS RIESGOS A LOS QUE SE ENFRENTAN LOS USUARIOS DE INTERNET EN ESPAÑA FRENTE A LOS ATAQUES Y VULNERACIONES DE CIBERSEGURIDAD. A PETICIÓN DEL GRUPO PARLAMENTARIO CONFEDERAL DE UNIDOS PODEMOS-EN COMÚ PODEM-EN MAREA. (Número de expediente del Congreso de los Diputados 219/000931 y número de expediente del Senado 715/000320).

El señor **PRESIDENTE:** Señorías, vamos a intentar seguir con un ritmo vivo.

Nos acompaña don Carlos Sánchez Almeida, director jurídico y miembro de la junta directiva de la Plataforma en Defensa de la Libertad de Información, para que evalúe los derechos a la libertad de expresión —siento que no esté el señor Mayoral, pero está bien sustituido— y de acceso a la información, así como los riesgos a los que se enfrentan los usuarios de Internet en España.

Tiene la palabra, por un tiempo de quince minutos, el señor Sánchez Almeida.

El señor **SÁNCHEZ ALMEIDA** (Director jurídico y miembro de la junta directiva de la Plataforma en Defensa de la Libertad de Información, PDLI): Buenos días, señor presidente.

Buenos días señorías. Ante todo, en nombre de la Plataforma en Defensa de la Libertad de Información, permítanme agradecer la invitación a esta Comisión Mixta Congreso-Senado de Seguridad Nacional, agradecimiento que les traslado también en nombre de su presidenta, Virginia Alonso, y de su secretaria general, Yolanda Quintana.

Si bien es la primera vez que hablo en esta casa, no es la primera vez que me dirijo a las Cámaras, ya que en otras dos ocasiones he hablado en el Senado. Repasando mi intervención en el Senado en el año 2001, me he encontrado con una cita de una sentencia del Tribunal del Distrito Oeste de Pensilvania,

cve: DSCG-12-CM-82

del año 1996, que considero fundacional en lo que se refiere al debate entre libertad de expresión y seguridad nacional. Esta sentencia del Tribunal del Distrito Oeste de Pensilvania, por un pleito que enfrentaba a la Unión Americana de Libertades Civiles con la fiscal general, Janet Reno, contra la Ley de Decencia en las Telecomunicaciones, que por aquel entonces impulsaba el Gobierno Clinton, que después sería confirmada por el Tribunal Supremo de Estados Unidos, tiene una serie de consideraciones sobre la libertad que a partir de ese momento iluminaron todo lo que fue el conflicto entre internautas, ciberactivistas y el poder gubernamental en diferentes escenarios. Dicha sentencia dice que Internet puede muy bien ser descrita como una conversación universal sin fin. El Gobierno no puede, a través de la Ley de Decencia en las Telecomunicaciones, interrumpir esa conversación. La ausencia de regulación gubernativa de los contenidos de Internet ha producido incuestionablemente una especie de caos, pero lo que ha hecho de Internet un éxito ha sido el caos que representa. La fuerza de Internet es ese caos. Como sea que la fuerza de Internet es el caos, la fuerza de nuestra libertad depende del caos y de la cacofonía de expresión sin trabas que protege la Primera Enmienda.

A partir de ese momento los activistas de Internet sabíamos lo que teníamos que decir —y lo hemos dicho en todas las ocasiones en las que hemos podido—: Que el único poder legitimado para intervenir en Internet en materia de contenidos en Internet ha de ser siempre el Poder Judicial. En el caso español ha de ser el Poder Judicial porque, en virtud del artículo 20 de nuestra Constitución, solo él puede secuestrar publicaciones, y toda Internet es una publicación, y solo él puede ordenar la interceptación de telecomunicaciones en caso de delito.

En diferentes campañas, en diferentes desafíos que hemos tenido los ciberactivistas españoles nos hemos encontrado con esta problemática. Ya en el año 2001 tuvimos un enfrentamiento pionero con el Gobierno de aquel entonces, porque pretendía aprobar una ley, la Ley de servicios de la sociedad de la información, que estaba en fase de anteproyecto, que permitía la intervención administrativa en materia de contenidos. Afortunadamente, en la tramitación parlamentaria, debido también a la presión de los ciberactivistas, se modificó el texto y se incluyó expresamente que para intervenir en Internet, para retirar contenidos de Internet, tenía que haber siempre autorización judicial. Esta polémica siguió en cada reforma de esta ley, porque también pasó con el siguiente Gobierno, el del señor Rodríguez Zapatero. Además, al final de la última legislatura del Gobierno Zapatero nos encontramos con una problemática, que fue otra vuelta de tuerca en la ley, lo que denominarían las redes la Ley Sinde, en cuyo anteproyecto se pretendía establecer una autoridad administrativa de control de contenidos. Finalmente, gracias a la intervención de otros partidos y a la presión de los ciberactivistas, hubo un pacto y se estableció un procedimiento judicial contencioso-administrativo de control de dichos contenidos.

En ese momento, además, surgió un manifiesto en defensa de los derechos fundamentales en Internet, que pueden leer en Wikipedia, impulsado, entre otras personas, por nuestra presidenta, Virginia Alonso, y todo cuando decíamos en él lo seguimos sosteniendo ahora, sobre todo por la experiencia que nos ha dado *a posteriori*, porque gran parte del ciberactivismo que se aglutinó en torno a la lucha contra la Ley Sinde también se aglutinó en los días del 15-M. Como consecuencia de ese desafío, del conflicto entre poder y sociedad —unos desafíos que en ningún momento cruzaron las líneas rojas del Código Penal, también hay que decirlo, porque lo que hicieron los internautas fue estirar al máximo lo que les permitía el ordenamiento—, han surgido nuevas iniciativas legales que han llegado al BOE y que han supuesto un retroceso de esas líneas rojas, que ahora están en otro sitio distinto —en perjuicio de las libertades— del que estaban cuando se producen los hechos del 15-M. Pienso que en buena parte, sobre todo por el cariz de las reformas, fue el 15-M, la posibilidad de la sociedad de utilizar redes telemáticas para aglutinar movilizaciones, lo que inspiró algunas de esas reformas.

Desde la Plataforma en Defensa de la Libertad de Información en todo momento hemos criticado estas leyes que, más allá de la Ley de Seguridad Ciudadana, que fue bautizada como Ley mordaza, conforman todo un cuerpo legislativo que podemos denominar también leyes mordaza. Entre estas leyes, en las que se introduce el control de contenidos de Internet, está la Ley de Propiedad Intelectual, la Ley de Seguridad Ciudadana, el Código Penal, la Ley Orgánica del Poder Judicial y la Ley de Enjuiciamiento Criminal. Todas ellas sufrieron modificaciones en la Legislatura 2012-2015 que han producido un retroceso de nuestros derechos. Buena parte de este retroceso ha sido denunciado en todo momento por la Plataforma en Defensa de la Libertad de Información, que se fundó en el año 2014, precisamente para hacer un seguimiento continuo de los ataques a la libertad de información y expresión en España. Esta plataforma ha realizado diferentes acciones de incidencia política, reuniéndonos con todos los partidos con representación parlamentaria: hemos hecho talleres de formación, en ocasiones de ciberseguridad,

cve: DSCG-12-CM-82

de uso de cifrado para periodistas, publicaciones divulgativas, análisis jurídico, campañas conjuntas con otras organizaciones internacionales, como el Instituto de Prensa Internacional, además de impulsar debates como, por ejemplo, en materia de noticias falsas, las *fake news,* tan de moda ahora. El primer acto sobre las *fake news* lo montó la Plataforma en Defensa de la Libertad de Información hace ya un año, en febrero de 2017. Posteriormente, también hemos impulsado un par de manifiestos en contra de las noticias falsas. Pueden encontrar ustedes en Google un manifiesto que se titula Diez fórmulas para hacer frente a las noticias falsas, que empieza diciendo que las noticias falsas son una amenaza para la libertad de información y para la democracia. Hay una serie de puntos en los que decimos que en todo momento debe llegarse a una definición consensuada de lo que son noticias falsas, que todos los actores de la cadena informativa están llamados a combatir y no fomentar la difusión de dichas noticias, que las obligaciones éticas y la deontología profesional del periodismo debe imponerse, que debe haber un periodismo de código abierto que pueda permitir la trazabilidad de las informaciones, precisamente para poder demostrar en todo momento la veracidad de las información, y que tiene que haber unas técnicas de verificación de contenidos que deben cumplir los estándares internacionales consensuados en la materia, entre otras, apartidismo e igualdad en la aplicación de técnicas de control de hechos.

De la misma manera, por lo que se refiere a las noticias falsas nuestra posición ha sido decir en todo momento que deben respetarse los estándares internacionales y que es muy peligroso que una autoridad gubernamental administrativa se arrogue la facultad de etiquetar, de señalar qué es falso y qué no lo es. Algo que debe decirse en todo momento es que la única verdad jurídica es la verdad establecida en sentencia judicial, el principio *res iudicata pro veritate habetur*. La otra verdad, la verdad histórica, siempre está sometida a discusión. No pasa como con la verdad científica, que es la única en la que realmente hay consenso.

Volviendo sobre la PDLI, quería aprovechar mi comparecencia hoy aquí para trasladarles algo que estamos diciendo desde la plataforma, sobre lo que decía antes de la reforma del Código Penal, y es que es necesario ver el problema que se ha producido al adelantar estas líneas rojas, porque conflictos que no llegaban a los tribunales están llegando, desgraciadamente está habiendo detenciones de tuiteros, de blogueros, incluso de periodistas. Pensamos que debe ponerse un poco de sentido común en lo que se refiere a los delitos de opinión. Cuando hablo de delitos de opinión me refiero a aquellos en los que el tipo penal se limita a lo que sería una manifestación de la opinión de una persona, pero es distinto cuando hay inducción al delito, cuando se incita a la discriminación, etcétera. Tenemos que ponernos de acuerdo en dónde está la línea roja, hasta dónde se puede regular, dónde tiene que empezar la libertad de expresión y dónde tiene que acabar el Código Penal. Es necesario que esta reforma del Código Penal se aborde por consenso, porque, en última instancia, lo que nos estamos jugando es el campo de juego. Las líneas que marcan el campo de juego donde están nuestras libertades son la libertad de expresión. La libertad de expresión es un derecho más que fundamental, porque es la garantía para el ejercicio de todos los otros derechos, por lo que entendemos que debe procederse a una reforma de acuerdo con los parámetros internacionales, de acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos, que ha dicho en repetidas ocasiones que en los casos de difamación no debe haber condenas de prisión. Discutiremos, en todo caso, si tienen que ser condenas de multa o tiene que llevarse al ámbito civil. Hay que ponerse de acuerdo.

Un debate sobre el que también quiero hablar es el del anonimato. El anonimato en Internet es consustancial al ejercicio de la libertad de expresión. Hay personas que no pueden decir lo que piensan si no utilizan un seudónimo. Este derecho al seudónimo no solo está reconocido en nuestras leyes, como en la Ley de Propiedad Intelectual, sino que, además, en el próximo Reglamento General de Protección de Datos, que entrará en vigor el 26 de mayo de este año, se establece el derecho a la seudonimización y también el derecho al cifrado, es decir, a ocultar, si queremos, nuestra identidad para pensar. Esto es algo que, repito, nos garantiza la propia normativa comunitaria, que establece, incluso, la posibilidad de que se sancione la reversión de la seudonimización cuando no ha sido autorizada por la persona.

También quiero hablar sobre los riesgos que comportan las noticias falsas y los ciberdelitos. En esta Comisión han tenido la oportunidad de escuchar a la fiscal especializada en delitos informáticos, en ciberdelincuencia, Elvira Tejada, quien les explicó la problemática de la investigación de los delitos en Internet. Algo que les dijo fue que en Internet absolutamente todo es rastreable, por lo que quien emite una noticia falsa, antes o después, va a tener que apechugar, va a ser señalado por otros medios de comunicación, que son su competencia, lo van a marcar para el futuro y van a decir: Este medio ha emitido noticias falsas en tal fecha, en tal fecha y en tal fecha. En caso de que las noticias falsas se emitan

cve: DSCG-12-CM-82

por agentes que no sean periodistas, que sean blogueros o tuiteros, también son rastreables. Se puede analizar el destino y toda la cadena de tuits. Cuando en Internet hay un linchamiento virtual, un acoso a una persona, que es delito, se puede rastrear y se puede dar con quien ha iniciado la cadena. Me permito sugerirles, porque sería muy interesante para los trabajos de esta Comisión, que sigan el trabajo de investigación de la doctora Mariluz Congosto, de la Universidad Carlos III, que lleva bastantes años analizando twitter y que con sus nubes de usuarios de twitter puede establecer sobre cualquier discusión que se produzca en la red qué partidos la están fomentando, qué medios de comunicación hay detrás, en última instancia, qué intereses hay detrás. Es muy interesante todo el trabajo que hizo sobre las movilizaciones del 15-M y posteriores, sobre las Mareas y demás. Sobre todas las olas que se han formado en Internet hay una trazabilidad, y en el trabajo de esta doctora lo tienen todo.

Deben tener en cuenta que en última instancia cada internauta es un verificador en potencia. Las mentiras en Internet tienen las patas muchísimo más cortas porque tenemos medios para rastrearlas, de la misma forma que tenemos medios para perseguir los ciberdelitos.

No quiero acabar esta comparecencia sin mencionar también una declaración conjunta sobre libertad de expresión y derecho a la información que han impulsado los relatores de libertad de expresión de la Organización de las Naciones Unidas, la OSCE, la OEA y ACHPR. Diferentes organizaciones internacionales nos dicen que efectivamente las noticias falsas son un peligro para las sociedades democráticas, pero que hay que ir con mucho cuidado a la hora de regular. En los principios generales, los relatores de las Naciones Unidas nos dicen que los Estados solo pueden imponer restricciones al derecho a la libertad de expresión de conformidad con el test para tales restricciones en virtud del derecho internacional, a saber: Que estén previstas en la ley, que sirvan a un interés legítimo y que sean necesarias y proporcionales. Por ejemplo, se puede prohibir la promoción del odio por motivos protegidos que constituya incitación a la violencia, la discriminación o la hostilidad. Sobre desinformación y propaganda, dicen los relatores de las Naciones Unidas que las prohibiciones generales basadas en ideas vagas y ambiguas, incluidas noticias falsas o información no objetiva, son incompatibles con las normas internacionales sobre libertad de expresión. También nos dicen que las leyes de difamación penales son indebidamente restrictivas y deberían ser abolidas. Los actores estatales no deben tampoco hacer, patrocinar, alentar o difundir declaraciones que ellos saben, o razonablemente deberían saber, que son falsas.

Nuestro Código Penal ya recoge las noticias falsas en varios apartados. Hay un delito que se ha aplicado en poquísimas ocasiones —estuve buscando jurisprudencia—, que es el de noticias falsas y rumores en materia de cotizaciones bursátiles. Lo que he citado es el artículo 284 del Código Penal. El artículo 561 dice que también se persiguen penalmente las falsas alarmas. También hay normas previstas sobre noticias falsas y propaganda en la Ley Electoral. La cuestión es si debemos hacer algo más o no. Considero que con lo que tenemos en el Código Penal en esta materia ya es suficiente, pero que en cualquier regulación debería tasarse claramente su finalidad. No puede hacerse una prohibición general de las noticias falsas, porque si lo hacemos, a lo mejor nos encontramos con que habrá autoridades y funcionarios que deberán ser procesados por emitir noticias falsas, por ejemplo, incluso notas de prensa policiales. Si posteriormente la sentencia desmiente completamente la versión policial y establece un relato de hechos probados absolviendo al acusado, podríamos encontrarnos con denuncias contra funcionarios o contra el *community manager* de la cuenta de twitter de la policía por haber emitido una noticia falsa. Esto es absurdo. Hay que ver que estamos en una nueva sociedad, que afortunadamente para todos el monopolio de la violencia solo lo tiene el Estado. Antiguamente, los Estados totalitarios tenían el monopolio de la propaganda, pero ese monopolio, afortunadamente, se perdió para siempre y no se lo vamos a devolver.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Sánchez Almeida.

Vamos a abrir ahora el primer turno de intervenciones de los grupos. Recuerdo a sus señorías que hemos acordado que el turno no exceda de cinco minutos. Les invito a ceñirse al tiempo.

Por el Grupo Mixto, tiene la palabra el señor Xuclá.

El señor **XUCLÁ COSTA:** Gracias, señor presidente.

Intervengo brevemente, en nombre del Grupo Mixto, Partit Demòcrata, simplemente para plantear al compareciente no una discrepancia, sino una reflexión sobre si no se tienen que prohibir o regular, mejor dicho, más cosas. Antes existía claramente una jerarquía de fuentes y de valoración de la calidad de las

cve: DSCG-12-CM-82

noticias. En un artículo de un periódico de papel el periodista tenía una semana para trabajar aquella información y publicarla, pero ahora hay una igualdad sin topografía de la calidad informativa, y un confidencial digital fabricado desde casa con una posverdad, digámoslo de otra forma, con una mentira colocada en un grupo de wasap, tiene unos efectos de difamación muy profundos.

En la legislación actual existe el derecho de rectificación que opera sobre la prensa escrita y los medios audiovisuales, y alguna vez hemos tenido que utilizarlo alguno de los aquí presentes para que se ajusten a la verdad. Pero con el mundo de los digitales ese derecho de rectificación no es operativo o bien se termina en los tribunales. Usted ha dicho que no es partidario de prohibir nada, y yo le digo que sería partidario de mejorar el derecho de rectificación, su impacto y su operatividad en el ámbito de los medios digitales.

Nada más. Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Xuclá

Tiene la palabra el señor Legarda.

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

Quiero dar las gracias al compareciente por sus explicaciones y por lo ilustrativo de su exposición. Le haré solo una pregunta. El fundamento —comparto lo que usted ha manifestado— es la libertad de expresión, que sobre todo es instrumental para la conformación de la pluralidad ideológica, que a su vez es una de las bases de una sociedad liberal democrática. Hasta ahí, estamos de acuerdo. La libertad de expresión da derecho a la pluralidad ideológica, es opinable si es acertada o desacertada, y también a la libertad de información, de eso no hay duda, que engloba la información equivocada. Pero lo que estamos tratando aquí es la información equivocada dolosa, hecha aposta. Desde su punto de vista, he entendido que lo ha matizado de una manera y luego de otra, ¿cree que la libertad de información dolosa debe atajarse o entra en la libertad de expresión?

Finalizo con un matiz. Usted ha apelado a un elemento de autorregulación que quizá fuera el más hábil para afrontar esta situación, pero siempre que hablemos de, digamos —entre comillas—, profesionales de la información. Hay mucha información, sobre todo a través de la TIC, y cada ciudadano puede convertirse en informador, porque no se necesita un medio de comunicación organizado, lo que era un periódico o un medio de comunicación tradicional. Esta autorregulación no la veo muy hábil para embridar esas otras fuentes de información no profesionales o no encuadradas en medios de comunicación.

Muchas gracias.

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

Tiene la palabra el señor Gutiérrez.

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

En primer lugar, señor Sánchez Almeida, muchas gracias por su comparecencia y su exposición. Plantea usted un debate que todos entendemos y que es precisamente el quid de la cuestión, es decir, dónde está ese limite entre la libertad, la seguridad y la protección del usuario o del consumidor, y también del actor que informa, comunica o escribe algo. Efectivamente, el Poder Judicial es el que tiene parte de la respuesta. No creo que usted encuentre en esta Cámara alguien que le vaya a decir lo contrario, porque aquí precisamente estamos para legislar, que es el trabajo que se hace desde el Congreso de los Diputados o, por lo menos, los grupos parlamentarios intentamos mejorar las leyes y, dentro del actual pluripartidismo, buscar el mayor consenso posible que es la nueva manera de entender la democracia en estos momentos.

En todo caso, abundando un poco en lo que comentaba el señor Legarda, usted se ha referido a la autorregulación, y dentro de los grupos editoriales, efectivamente, el profesional se puede someter a esa autorregulación porque está trabajando en un sitio determinado, se identifica como profesional, y tiene unas credenciales, una opinión o un espacio público que debe defender. Esto lo entiendo y creo que es un camino, pero dejamos fuera un ámbito muy importante que es la opinión personal. Hoy en día cualquiera puede manifestar su opinión porque es muy fácil abrir un blog y hacer un comentario sobre lo que uno quiera. Esa autorregulación es tanto como decirle a la gente que sea buena, que está muy bien, es muy bonito y simpático, pero la realidad es que si esto fuera así, entonces no harían falta los jueces, no necesitaríamos para nada el Poder Judicial. Bien, el Poder Judicial y las Fuerzas y Cuerpos de

cve: DSCG-12-CM-82

Seguridad del Estado están precisamente para proteger a los ciudadanos de estas cosas. Por tanto, es cierto que este debate está encima de la mesa, es sano y es el momento en que se debe plantear.

También hay que distinguir algo que vemos todos los días, los delitos de odio, que cada vez están teniendo más importancia. Me parece que el delito de odio al final es un delito y el canal por el que exprese es lo de menos; es un delito y como tal debe ser perseguido, sentenciado y aplicarse la sanción correspondiente. Si esto entra dentro del ámbito penal o administrativo, efectivamente ese es el debate porque es muy difícil situar la delgada línea entre el derecho individual de la libertad de expresión y lo que puede constituir un delito, y a lo jueces en muchas ocasiones les ponemos las cosas muy complicadas a la hora de valorarlo. Estamos viendo esto todos los días sin necesidad de hablar de Internet, también pasa en otras actividades comunes; por ejemplo, dónde hay un delito de odio cuando se convoca una manifestación y allí se dicen una serie de cosas. Muchas veces los jueces no entran a valorar si existe ese delito de odio. Lo estamos viendo estos días en el País Vasco perfectamente, cómo se hacen recibimientos a etarras contra las víctimas del terrorismo y se hace apología de ese odio, y los jueces no entran a valorar nada porque entra dentro del ámbito de la libertad de expresión. Creo que esto es algo que tenemos que regular y, a lo mejor, es un acierto situarlo en el ámbito administrativo. Por eso digo que el canal es independiente, creo que existe un debate en la sociedad sobre cuál es la diferencia entre la libertad de expresión y la seguridad o la protección del resto de los ciudadanos, y está muy bien que hablemos de eso.

Luego tengo una duda que me gustaría plantearle, porque aquí, en España, tenemos una responsabilidad respecto a nuestro Poder Judicial, pero qué pasa cuando esos delitos de odio provienen de otro sitio, cuando esas noticias falsas que usted está comentando vienen de otros países o de otros espacios. Y quizás volvemos a entrar en el debate anterior sobre la gobernanza local, global, de qué forma se comparte esa gobernanza, y de qué manera esa gobernanza tiene la responsabilidad de que lo que se esté haciendo sea conforme a la ley —digamos universal—, aunque ya sabemos que los delitos de odio no son iguales en cada país. En fin, estas son las cuestiones que quería plantearle y, de nuevo, le agradezco su presencia.

Muchísimas gracias.

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

Tiene la palabra el señor Del Olmo.

El señor **DEL OLMO IBÁÑEZ:** Gracias, señor presidente.

Señorías, actualmente en esta Comisión se está analizando el fenómeno de la desinformación y, por esta razón, hemos solicitado la comparecencia de Carlos Sánchez Almeida, director jurídico y miembro de la Plataforma en Defensa de la Libertad de Información. Así que lo primero es volver a darle la bienvenida y agradecer su participación al compareciente. En todo este periodo se está produciendo en esta Comisión una confusión muy grave, que puede venir por desconocimiento o por las ganas que tienen algunos de meterle mano a la libertad de expresión; se están equiparando los conceptos de ciberguerra y desinformación. Y la diferencia no es menor, por un lado, la ciberguerra es una ofensiva dirigida a tumbar infraestructuras estratégicas o a robar información, y por otro, la desinformación es la acción o efecto de desinformar que puede consistir, uno, en dar información falsa o manipulada de manera intencionada y, dos, omitir información o dar información insuficiente. Son dos cosas muy diferentes, señorías.

Aunque es un problema que hay que abordar, 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. Según mis cálculos, en España seguro que una parte importante de este 1 % corresponde al medio de comunicación de Eduardo Inda, *Okdiario*, por cierto, financiado con 300 000 euros de dinero público. Pero volvamos al tema, el Centro Criptológico Nacional —organismo adscrito al Centro Nacional de Inteligencia, CNI—, 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 crisis catalana. Así que se pueden quedar tranquilos los que han alimentado esta alarma como, por ejemplo, Ciudadanos, que el 15 de noviembre, justo antes de las elecciones en Cataluña, preguntaba al Gobierno aquí en el Congreso sobre las medidas para evitar que los rusos sabotearan mediante *hackers* los comicios del 21 de diciembre. Primera pregunta para el compareciente, ¿es un error equiparar los conceptos de ciberguerra y desinformación?

cve: DSCG-12-CM-82

Si hablamos de desinformación en España, lo primero de lo que tendríamos que hablar no es de las redes sociales, como hace la mayoría de partidos aquí; tendríamos que hablar de Televisión Española, la televisión pública que el Partido Popular maneja como si fuese la televisión de su partido. Hace unas semanas, el telediario de Televisión Española en una de sus ediciones contaba que el Partido Popular había sido encausado por la destrucción de los ordenadores de Bárcenas, aunque estos ordenadores —decían en el telediario— no contenían información relevante. Pero vayamos un pasito más, la señora De Cospedal, ministra de Defensa, dijo el pasado mes de noviembre: Voy a proponer a la Comisión de Defensa del Congreso la creación de un grupo de trabajo que reúna a diputados y editores de los principales medios de comunicación, para estudiar a fondo la amenaza de la desinformación contra nuestra democracia. Pregunta para el compareciente, que sea un Gobierno el que decida qué información es falsa y cuál no, ¿no sería peligroso para la libertad de expresión y para el derecho a la información? Los de la manipulación en Televisión Española, los de las armas de destrucción masiva que había en Irak, los que contrataban a Alejando de Pedro, el conseguidor de la trama Púnica, para que hiciera campaña en redes sociales para mejorar la reputación de Esperanza Aguirre o cargar con informaciones falsas sobre la marea verde; estos mismos quieren ser los que pongan un sello a la información para decir a los ciudadanos cuál es buena y cuál es mala. La señora De Cospedal lo que quiere es crear el ministerio de la verdad, seamos claros. Me van a permitir que yo en esta cuestión esté más cerca de la vicepresidenta, Soraya Sáenz de Santamaría, y voy a intentar explicarme. La vicepresidenta ha abandonado a la señora De Cospedal en su intento de crear un órgano de censura política, apostando por la educación y la información rigurosa. Y es que la señora De Cospedal no quiere entender que la desinformación se combate con más y con mejor información y no con censura, como hacía ella en la televisión pública de Castilla-La Mancha. Comenzó hace unos meses, con aire de película mala de guerra fría, una campaña para crear una alarma sobre una supuesta injerencia rusa en España a través de las redes sociales. Y sobre esas injerencias para desestabilizar la democracia en España, hemos vivido aquí en la Comisión grandes momentos; el señor Hernando, del Grupo Parlamentario Socialista, la comparó con un pato, la señora Milosevich, de la Fundación FAES, a la que todo el mundo aquí hizo la pelota, dijo que no tenía pruebas, pero que había leído algo en no sé qué periódico. También fuera de esta Comisión, hemos visto en el Parlamento británico a tres aventureros que, en nombre de España, fueron a contarles que no había pruebas de la injerencia rusa, pero que de algo de esto se habían enterado en algún viaje a no sé qué otro país. Con todas estas pruebas, señorías, y esta seriedad, no sería extraño que en su próxima ocurrencia le quisieran cambiar el nombre al CNI y pasar a llamarlo como aquella famosa agencia de Mortadelo y Filemón, la de los Técnicos de Investigación Aeroterráquea.

Señorías, quizás el problema no sea la amenaza rusa, quizás lo que hay detrás de esto es una operación para generar miedo y poder restringir derechos y libertades, aplicar una Ley mordaza 2.0. Para terminar, le formularé una última pregunta. El Gobierno ha anunciado que quiere prohibir el anonimato en las redes sociales. ¿Piensa usted que el Gobierno vulneraría el derecho a la intimidad si obliga al usuario a identificarse parcialmente o en su totalidad en las redes sociales?

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Del Olmo, por esta omnicomprensiva intervención.

Voy a dar la palabra ahora a la señora Botella.

La señora **BOTELLA GÓMEZ:** Muchas gracias, señor presidente.

Doy las gracias al señor don Carlos Sánchez Almeida, el compareciente en esta sesión. En primer lugar, si me permiten, voy a intentar centrar de nuevo el tema hacia el objeto de esta Comisión. Es la primera vez que comparezco en esta Comisión, y he tratado de entender el estado de situación de la problemática que queremos reflejar, porque estoy adscrita a esta Comisión Mixta de Seguridad Nacional para el informe de la ponencia y nos interesa mucho aprovechar la visita de expertos, como es su caso, para ir directamente al núcleo duro de la tarea de esta Comisión. En ese sentido, he escuchado su intervención y también he visto que usted ya había comparecido en el Senado hace diecisiete años —en 2001, tan reciente y tan lejano, el tiempo vuela—, y entonces ya cito muchas de las problemáticas —aunque no con los mismos nombres, por ejemplo, la palabra ciberseguridad no aparece en ese documento— de este debate que es muy riguroso y de mucho calado. Lo podemos salpimentar ahora con muchos casos de la política nacional, pero creo que no procede, y debemos ir directamente a cuáles son las competencias legislativas que nosotros tenemos aquí, cuál es nuestra responsabilidad para facilitar su trabajo a los jueces. Según mi apreciación, usted ha insistido mucho en que sean los jueces los que

cve: DSCG-12-CM-82

sancionen, cuando en realidad tenemos dos caminos intermedios que son responsabilidades, una responsabilidad es directamente nuestra y otra del Ejecutivo. Una es que las leyes sean suficientemente claras, modernas, actualizadas, homologables a la mejor legislación, buenas prácticas y experiencias internacionales, normalmente europeas que es nuestro ámbito normal de relación. Y otra responsabilidad es que haya organismos con una capacidad técnica, con independencia, como también se ha citado, que puedan verificar exactamente las cuestiones técnicas tan complejas en este mundo de la ciberseguridad, de modo que cuando haya un litigio y llegue a los jueces o magistrados sea mucho más clara su determinación.

De todas maneras, me ha llamado simpáticamente la atención que usted, no sé si consciente o inconscientemente, se haya declarado como activista en Internet. Creo que es una oportunidad que comparezcan personas con un perfil jurídico y, a la vez, con ese activismo en Internet. En la petición de comparecencia había dos partes, y usted se ha centrado exclusivamente en una, en los derechos de libertad de expresión y de acceso a la información, pero ha soslayado los riesgos a los que se enfrentan los usuarios de Internet en España frente a los ataques y vulneraciones de ciberseguridad. A nosotros sí nos interesa tener esa visión de conjunto. Entonces, permítame que le haga alguna reflexión al respecto. ¿Por qué los riesgos son acotados solo a los usuarios de Internet y en España? Normalmente en las comparecencias estamos viendo que el riesgo es global, que la amenaza no solamente es en España, que lo que ocurre en España puede venir de otros ámbitos geográficos y destinos, y que además no está acotado solo a los usuarios cibernautas, sino que el más común de los ciudadanos, en un pueblecito de Soria o de mi comunidad, la Comunidad Valenciana, puede verse afectado sí o sí, aunque no sea un usuario de Internet si, por ejemplo, caen las instalaciones críticas, si caen los hospitales, etcétera. En ese sentido le pregunto si debemos trabajar a escala nacional o a escala europea. Desde su experiencia jurídica y también desde su activismo en Internet, para la resolución de los problemas en los que nosotros como legisladores nos vamos a tener que centrar, ¿debemos valorar las experiencias europeas como, por ejemplo, las estrategias que hay ahora mismo, esa estrategia que el anterior ponente también ha destacado, la directiva NIS que vamos a tener que trasponer, la Agencia Enisa que ya está funcionando en la Unión Europea o esas directivas que van hacia un espacio determinado? Incluso se habla de un mercado único europeo de la ciberseguridad, de los derechos de los usuarios y de los derechos europeos en la ciberseguridad. Como jurista, ¿cree usted que debemos prestar atención a lo que se está haciendo en el exterior o debemos enfocarnos mucho más en nuestra legislación nacional, trasponer lo justo y centrarnos más en nuestra idiosincrasia?

Por otra parte, qué opinión le merece la idea de esa fragmentación —que estamos viendo en las distintas comparecencias— de las diferentes competencias que tenemos en España. Esto también es materia legislativa por las leyes que tienen que ejecutar los distintos ministerios. Tenemos muchos ministerios y algún organismo de coordinación, pero quizás no con las dotaciones suficientes para tener una competencia propia, por ejemplo, el Consejo Nacional de Ciberseguridad, que se ha montado sobre la base de la coordinación de todos los ministerios, pero no tiene la estructura de una agencia que pudiera centralizar y ser un punto de referencia. Entonces, tenemos el Ministerio del Interior, el Ministerio de Defensa, el Ministerio de Industria y el Ministerio de Educación, que también debería entrar por el tema de la educación digital. ¿Cree usted que toda esa fragmentación ocasiona daños que luego ustedes están viendo en el ámbito jurídico? Nosotros, desde el Poder Legislativo, ¿deberíamos impulsar medidas de organización y mayor coordinación para ser más operativos? Por ejemplo, en el caso de LexNET y el fallo de seguridad tan grave que se produjo, dejando desprotegidos miles de archivos y documentos de particulares en el ámbito de la justicia, con más de 3000 órganos judiciales afectados, ¿estamos preparados para gestionar esta Administración electrónica, este salto a esa economía digital? ¿Cómo conciliar en este caso el derecho de los afectados y la responsabilidad que tienen las autoridades públicas? Es decir, pasa el fallo, se cierra la solución, ¿y luego qué pasa, qué responsabilidades hay?

Al hilo de este último comentario, me interesa la atribución de responsabilidades en relación con el anonimato. Me gustaría que usted diera un paso más, fuera más explícito y se pronunciara en ese debate sobre el bien jurídico a proteger entre la libertad de expresión y la seguridad. El anonimato está en el núcleo duro de algunos de los problemas con los que nos hemos enfrentado. Y no coincido con usted en el tema de la trazabilidad. Yo no soy una experta, pero por lo que he podido leer, técnicamente no parece que sea tan fácil esa trazabilidad. De hecho, cuando se habla de los ataques a Cataluña, no se pueden demostrar porque hay vías indirectas por las que pueden haber llegado. Se hablaba de Venezuela, de los robots que enviaban la información. Entonces, a nivel nacional es difícil, y a nivel internacional todavía es

cve: DSCG-12-CM-82

más difícil porque ya entran países con unas competencias, unos medios y unos mecanismos que nos desbordan. En ese sentido, ¿cuál considera usted que es el bien jurídico a proteger de cara a la seguridad? Hablamos no solo de los internautas, sino de todos los ciudadanos.

Por último —ya termino—, creo que algunas cuestiones que ha comentado corresponden más al ámbito de la Comisión de Justicia, por ejemplo, la reforma del Código Penal, los delitos de opinión. Respecto a las noticias falsas, ¿hay algo que nosotros podamos hacer aquí en el Parlamento porque considere usted que está en nuestras manos legislar sobre ello? Tenemos registradas proposiciones no de ley de diferentes grupos parlamentarios. El Parlamento británico está dando un ejemplo de rapidez, que puede ser más o menos cuestionable, pero lo cierto es que realmente se ha puesto a trabajar específicamente sobre este tema de la desinformación. Las declaraciones de la ministra española quizás son un poco superficiales, porque no tiene sentido hablar de un grupo de trabajo en un Parlamento cuando hay subcomisiones e instrumentos más garantistas para establecer la forma en que se podría hacer. En su opinión, para neutralizar esta problemática, ¿qué podríamos hacer o impulsar desde el Parlamento?

Muchísimas gracias.

El señor **PRESIDENTE:** Muchas gracias, señora Botella. No lo he hecho antes, pero aprovecho para darle la bienvenida a esta Comisión. Y quiero decirle que, en mi opinión, aunque serán los grupos parlamentarios los que lo decidan, la ponencia sobre ciberseguridad tendrá el ámbito objetivo que nosotros decidamos, con independencia de que las recomendaciones luego sean estudiadas por las Comisiones pertinentes en cada área. Nadie nos ha puesto límites y, por lo que yo preveo, nadie nos los va a poner en el futuro.

Ahora, por el Grupo Parlamentario Popular, tiene la palabra el señor Cosidó Gutiérrez.

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

En nombre de mi grupo, manifiesto nuestro agradecimiento al compareciente por su aportación. No es fácil abordar una cuestión como es la libertad de expresión y de información en cinco minutos, pero haremos algunas preguntas y alguna reflexión añadida a la comparecencia. Como ha habido otros grupos que no han utilizado todo el tiempo, a lo mejor tenemos por parte del presidente un pelín más de flexibilidad. Hablamos de libertad de expresión y libertad de información en un nuevo entorno tecnológico, de un pilar básico del funcionamiento de nuestra democracia, de dos libertades esenciales en la propia definición de democracia. Me gustaría empezar dando una visión positiva del impacto que las nuevas tecnologías han tenido sobre la libertad de expresión y también sobre la libertad de información, sobre la accesibilidad de los ciudadanos a la información. Creo que Internet y las redes sociales nos dan más libertad, han aumentado el grado de libertad en el mundo y también en España. Además, creo que nos dan más transparencia y más capacidad para el control de los poderes públicos, así como más acceso a la información, especialmente de las administraciones públicas por parte de los ciudadanos. Ahí está la Ley de transparencia, acceso a la información pública y buen gobierno, que es uno de los ejemplos más avanzados en el mundo en cuanto a garantizar ese derecho de accesibilidad a la información. No sé si el compareciente coincide con esta visión positiva. Y también creo que tenemos un problema, y es que en Internet encontramos cada vez —si me permiten la expresión, que es muy burda y pido que no me malinterpreten— más basura; encontramos más discursos de odio racial, más pornografía infantil, más daños al honor y a la intimidad de las personas, y ahí están fenómenos como el ciberbullying, que es un buen ejemplo de cómo las nuevas tecnologías siendo muy positivas para la libertad de expresión y la libertad de información, tienen también un riesgo en cuanto a la protección de derechos fundamentales de las personas, que es en definitiva lo que en esta Comisión y en esta ponencia vamos a intentar equilibrar de alguna manera.

Quisiera hacer también una referencia a que no estamos ante un debate español, esta es una cuestión que afecta al conjunto de la comunidad internacional. Sé que lo conoce bien, pero me gustaría citar el artículo 10 del Convenio Europeo de Derechos Humanos, cuando establece que el ejercicio de estas libertades —la libertad de información y la libertad de expresión—, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del Poder Judicial. Este es el Convenio de Derechos Humanos del Consejo de Europa. Lo digo también porque,

cve: DSCG-12-CM-82

según algunas intervenciones, parece que aquí había una coartada para utilizar y restringir las libertades en nuestro país. No, mire usted, este es un debate que afecta al conjunto de la comunidad internacional. En nuestro ordenamiento creo que la cuestión está bien orientada y muy bien perfilada en el artículo 20.4 de nuestra Constitución, que es la que en definitiva garantiza nuestros derechos al establecer que las libertades reconocidas en este artículo, relativo a la libertad de expresión, tienen su límite en el respeto a los derechos reconocidos en el Título I de la Constitución española, en los preceptos de las leyes que los desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. Por tanto, todos coincidimos en que es un derecho esencial y básico de nuestra democracia, pero no es un derecho ilimitado, tiene límites que están claramente reconocidos tanto en la doctrina internacional como en nuestra propia Constitución.

Hecho este preámbulo, que yo creo que no admite mucha discrepancia, aunque siempre hay algún grupo que puede plantear alguna, me gustaría preguntarle si en lo que definimos como periodismo ciudadano, que es esta posibilidad de información nueva que se abre a través de las redes sociales, blogs o cualquier tipo de instrumento en Internet, en su opinión, ¿el nivel de exigencia y responsabilidad es equiparable al de los medios más tradicionales, o cree que debemos tener un marco diferenciado para lo que definimos como periodismo ciudadano o periodismo profesional —entre comilllas—, si es que lo podemos definir así? En segundo lugar, cuando alguien tiene una cuenta en redes sociales, lo que ahora nuestros adolescentes llaman *influencers,* con miles de seguidores, quisiera saber si, a efectos de posible exigencia de responsabilidades, ¿debemos considerar esto como medio público o lo debemos mantener en una esfera puramente privada y, por tanto, en otro nivel? En tercer lugar, a pesar de que algún grupo, sorprendentemente, niega la existencia de las *fake news,* creo que es una realidad constatada que ha habido claramente campañas de desinformación; en las elecciones en Estados Unidos, en el referéndum del *brexit* británico y, con mucha unanimidad en la comunidad internacional, en el caso de Cataluña en España y, por tanto, creo que España objetivamente también ha sido víctima de estos ataques, como otras muchas democracias en el mundo, es decir, en esto tampoco somos muy distintos. Usted ha dicho que lo mejor en este terreno es no hacer nada. Yo creo que algo tenemos que hacer, no sé muy bien y exactamente qué es lo que tenemos que hacer, pero me parece que nuestras democracias no pueden permanecer impasibles. Ninguna gran democracia del mundo está de brazos cruzados ante ataques de esta naturaleza. Esto si entrar en la procedencia de los ataques, porque es cierto, como también se ha puesto de manifiesto, que en Internet aunque siempre hay trazabilidad, en ocasiones llegar al origen de quién está detrás de esas informaciones es enormemente complejo y más en un marco internacional.

Por otro lado, coincido con una afirmación que usted ha hecho, y también he escuchado a la portavoz del Grupo Parlamentario Socialista, sobre la importancia de la educación, es decir, alguna forma de alfabetización digital, especialmente para nuestros menores, que les permita tener criterio y saber diferenciar lo que es verdad de lo que es mentira, y también los riesgos que en muchas ocasiones tiene la utilización de estas nuevas tecnologías. Me gustaría que nos diese alguna indicación sobre qué se plantean ustedes en el ámbito de la formación o educación de los ciudadanos en esta materia. He hablado de los menores, pero probablemente sea una labor para toda la sociedad. Por otra parte, sí creo que hay una diferenciación entre el derecho a la información y la libertad de expresión. Esta es quizás una discusión un tanto doctrinal que trasciende lo que hoy estamos debatiendo, pero creo que en la libertad de expresión no hay una obligación de veracidad. Es decir, uno puede expresar lo que quiera independientemente de que sea verdad o sea mentira, no hay una obligación de que uno tenga que expresar necesariamente la verdad. En todo caso, no decir la verdad no es punible ni sancionable, ni siquiera desde el punto de vista administrativo. Pero en el derecho a la información sí que hay un deber de veracidad. Es decir, los ciudadanos sí tienen un derecho a recibir una información veraz. Por tanto, esa es una responsabilidad que afecta también a los poderes públicos y nos afecta a los legisladores, cómo garantizamos que los ciudadanos tengan una información veraz sin que eso colisione con ese otro principio fundamental que es la libertad de expresión, que también debemos garantizar en todo momento.

En definitiva, el problema es complejo, sobre todo porque las nuevas tecnologías nos abren un horizonte nuevo y un nuevo campo de juego, en el que probablemente es necesario redefinir algunas de las reglas del juego que habían funcionado para los medios tradicionales, pero la esencia, al menos en mi opinión, sigue siendo exactamente la misma: máximo respeto a la libertad de expresión, pero no podemos amparar expresiones o informaciones que afecten a los derechos fundamentales de otros. Esto es verdad en cualquiera de los ámbitos o medios en los que nos movamos.

cve: DSCG-12-CM-82

Esto me lleva a una penúltima consideración. Es adelantar mucho, porque ya llegarán las conclusiones de la ponencia y es lo que estamos debatiendo y estudiando, pero después de escucharle a usted y a algunos grupos diría que esta es una materia en la que no es fácil legislar, en la que debemos movernos con mucha prudencia, porque hay derechos fundamentales que en ocasiones pueden estar en juego, pueden estar en litigio. Por tanto, no es por escurrir el bulto, en absoluto, pero creo que una parte muy importante en la solución de este tipo de conflictos y de debates lo va a tener el ámbito jurisdiccional. Es decir, como no puede haber principios únicos sobre lo que es verdad y no es verdad en lo que afecta o no afecta a derechos fundamentales de otros y prima la libertad, en muchas ocasiones tendrán que ser los jueces los que decidan si en ese caso hay un delito de exaltación del terrorismo, de humillación a las víctimas, que, en absoluto, puede estar amparado por el derecho a la libertad de expresión, o si en referencia a ese caso hay sentencias en España sobre alguien que ha publicado el anagrama de ETA o ha sacado la foto de un terrorista pidiendo su libertad y el Tribunal Supremo lo ha absuelto porque ha considerado que en ese caso no había estrictamente un delito de exaltación del terrorismo y, por tanto, estaba amparado por la libertad de expresión. En otros casos —y algunos se han puesto de manifiesto en esta comparecencia— los jueces han determinado que sí existía un delito que afectaba a derechos fundamentales y, por tanto, han hecho una sentencia condenatoria. Aquí es fácil también hacer demagogia: no por un tuit, sino por haber vulnerado derechos fundamentales de las víctimas o haber cometido un delito de exaltación del terrorismo, que es un delito especialmente grave en nuestro ordenamiento jurídico.

Termino, señor presidente —creo que me he atenido más o menos al tiempo—, también reafirmando una cuestión de principios. Creo que nuestra democracia, la democracia española, que ahora cumple cuarenta años, no es perfecta, porque no creo que exista ninguna democracia en el mundo que sea perfecta, pero tenemos una democracia de buena calidad, y discrepo de aquellas posiciones —creo que el compareciente ha estado muy equilibrado en su intervención— que ponen en cuestión que tengamos un problema de calidad democrática, que nuestro país sea equiparable a otros países en los que la libertad de expresión sí está seriamente comprometida. Creo que tenemos un ordenamiento que garantiza muy razonablemente la libertad de expresión en este equilibrio con los derechos fundamentales de otros, y no creo, en absoluto, que en nuestro país estemos en un proceso de recesión de libertades democráticas. Más bien al contrario, creo que todos —y esta comparecencia estoy convencido de que contribuirá a ello— estamos en una fase de expansión de nuestros derechos, de nuestras libertades, porque las nuevas tecnologías nos ofrecen nuevas oportunidades también en ese terreno, como ya he señalado.

Muchas gracias, señor presiente. **(Aplausos).**

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

Tiene la palabra el compareciente por un tiempo estimado de cinco minutos para contestar a las distintas preguntas formuladas.

El señor **SÁNCHEZ ALMEIDA** (Director jurídico y miembro de la junta directiva de la Plataforma en Defensa de la Libertad de Información, PDLI): Muchas gracias, señor presidente.

Voy a intentar ajustarme al tiempo de cinco minutos, pero ya les digo y les avanzo que han sido mucho más interesantes las preguntas que ustedes han hecho que las respuestas que yo les pueda dar. Intentaré ir por orden, contestando a cada uno de las personas que han intervenido.

En primer lugar, el señor Xuclà hablaba de la jerarquía de fuentes de información que antes representaban los periódicos, de que ahora estamos en una situación de igualdad y de si tenemos que modificar nuestras leyes sobre difamación para incluir a medios digitales. Ya están incluidos esos medios digitales. Tengo incluso experiencia, en ocasiones he tenido que defender en tribunales a algunos precisamente porque se ha ejercitado frente a ellos el derecho de rectificación. Es una cuestión sobre la que en cierta medida ha habido un hilo conductor entre todas las intervenciones. Precisamente, el señor Cosidó, al final, también lo consideraba, si se tiene que aplicar la misma ley a medios de Internet y a medios tradicionales. Y lo cierto es que para determinados delitos, como, por ejemplo, el que comentaba de enaltecimiento del terrorismo, es el propio Código Penal el que pone al mismo nivel los dos medios. Dice que la difusión en Internet o en medios de comunicación aumentará la pena. Entonces, pienso que quizás habría que ponderarlo en futuras intervenciones legislativas y habría que atender, sobre todo, incluso a la hora de castigar o de establecer indemnizaciones, a la difusión que ha tenido esa información perjudicial, esa información dolosa, esa información difamatoria. Habría que atender a la verdadera difusión. Y de la misma manera, volviendo a los delitos de enaltecimiento del terrorismo, también hay que tener en cuenta —ya lo está teniendo en cuenta el Tribunal Supremo, que está cambiando su jurisprudencia

cve: DSCG-12-CM-82

en estos días— la verdadera difusión del mensaje. Un tuit que no tiene retuits, ¿a quién causa daño? Por mucho daño que quiera causar el autor, estamos hablando de un delito imposible.

Ha dicho el señor Legarda que habría que garantizar la pluralidad ideológica, que es la base de la libertad de expresión, pero cuestiona qué hacemos con la información dolosa, si se deben regular los profesionales, si debe haber autorregulación o si dejamos esa autorregulación en manos de los usuarios. Pienso que la autorregulación es buena para determinadas situaciones pero que para otras tiene que estar tasado en la ley, y la ley es igual para todos. Vuelvo a insistir en que tiene que haber considerandos en esa ley precisamente para los casos en los que no ha habido una difusión real. En esos casos no puede ser la misma sanción a un medio digital, a una página web, a un blog, a una cuenta de Twitter, no se puede poner al mismo nivel que a un periódico de difusión nacional. Habrá que ver en cada caso las circunstancias.

Decía el señor Gutiérrez que el Poder Judicial ha de ser la respuesta. Evidentemente, en delitos de odio no puede haber otra respuesta que el Poder Judicial, o sea, no tiene que haber una intervención administrativa en delitos de odio. Pero se nos preguntaba también si tenemos que acudir a la legislación internacional, si se tiene que regular en España —creo que era la señora Botella quien lo preguntaba— o si simplemente tenemos que limitarnos a transponer los convenios internacionales. Creo que cada vez más vamos en el ámbito europeo hacia una uniformidad legislativa y pienso que tenemos que estar a que se cumpla sobre todo esa normativa europea. Antes les hablaba del Reglamento General de Protección de Datos, que entrará en vigor el 26 de mayo. Es un caso de aplicación directa de normativa comunitaria, a lo que nos tendríamos que ir acostumbrando. Y pienso que todo este debate, incluso el de las *fake news,* debe ser llevado al ámbito europeo. Innovar legislativamente en una materia como esta solamente en España supone correr riesgos innecesarios de acabar siendo condenados por el Tribunal Europeo de Derechos Humanos. Pienso que es mejor estar a la normativa europea, como ya se ha hecho, por ejemplo, en ciberdelitos con el Convenio de Budapest —lo recordó la fiscal de delitos informáticos—, y pienso que ha de ser una normativa europea la que lo controle.

El señor Del Olmo me preguntaba si es un error equiparar ciberguerra y desinformación. Sí, por supuesto que es un error, cada cosa es distinta. Quiero aprovechar para recomendarles un libro muy interesante sobre ciberguerra que escribió precisamente nuestra secretaria general, Yolanda Quintana, que está hoy en esta sala. Recomiendo la lectura de este, junto con la del libro Ciberactivismo, de la misma autora, porque explica a las claras lo que es la ciberguerra, que es una cosa muchísimo más seria, como ya, por otra parte, les explicó el general experto en ciberseguridad que estuvo en esta Comisión. La ciberguerra y las ciberarmas son una cosa muy seria. Y sobre el tema de las *fake news* y el conflicto en Cataluña, soy de los que piensan que el tema de la ciberguerra hay que dejarlo completamente al margen; el fenómeno es otro —ahora lo hablaremos—. De todas maneras, la desinformación sigue siendo también un peligro. No es ciberguerra y hay que atajarla de otra manera. Así como la ciberguerra debe ser responsabilidad de los profesionales de la guerra, la desinformación ha de ser responsabilidad de los profesionales de la información.

Sobre el tema referente a la televisión pública, la verdad, señor Del Olmo, no voy a opinar sobre la televisión pública, ni sobre la de aquí ni sobre la de Cataluña, porque no las veo. Ha llegado un punto —y como yo muchos internautas— en que solo consumo televisión vía Netflix, precisamente para evitar problemas, entre otras cosas porque además la mayor parte de la información ya la recibimos por Internet.

Sobre el ministerio de la verdad, la injerencia rusa, el pato que hace cuá, cuá, del que se habló en otras sesiones de esta Comisión y demás, realmente, he defendido en muchas ocasiones a personas acusadas injustamente de ser *hackers*. Precisamente hoy he coincidido con el señor Mitxelena, que me ha precedido. Recuerdo que allá por el año 2000 tanto él como yo íbamos reclutando *hackers* españoles para trabajar en ciberseguridad, para pasarlos al lado bueno, por así decirlo, y tengo alguna experiencia con ellos. Los mejores, algunos que eran perseguidos a finales de los noventa han acabado asesorando a Microsoft y Google. Entonces, tenemos *hackers* tan buenos aquí que no necesitamos para nada a los *hackers* rusos, de verdad. Cuando se me habla de estos, me acuerdo de los chistes de Eugenio, de ese que dice: Mucho ruso en Rusia y muy buena la ensaladilla rusa. Cuando hay *hackers* en España, cuando son verdaderos *hackers,* cuando realmente han cometido un delito, están los jueces y están las brigadas especializadas para detenerlos. Y hay trazabilidad, les he dicho en todo momento que hay trazabilidad en Internet, que se detiene a las personas. Y lo que ha pasado, por ejemplo, en Cataluña cuando se ha investigado sobre esta gente que replicaba la web del referéndum y demás, lo que han encontrado los jueces y los policías es que eran personas de aquí, no eran *hackers* rusos los que estaban subiendo

cve: DSCG-12-CM-82

aquellos contenidos. Por tanto, entiendo que hay que acudir a esta facilidad de Internet para trazar la información y dejarnos de cosas no probadas, porque la única verdad establecida es la verdad judicial, y lo que salga en esas sentencias ya lo veremos. De momento, no han imputado a ningún *hacker* y, sin embargo, sí han imputado a muchas personas de aquí.

Gracias.

El señor **PRESIDENTE:** Gracias.

Abrimos un segundo turno de portavoces y seguimos el mismo orden.

¿Va intervenir el señor Xuclà? **(Denegación).**

¿El señor Legarda? **(Denegación).**

¿El señor Gutiérrez? **(Denegación).**

Tiene la palabra el señor Del Olmo.

El señor **DEL OLMO IBÁÑEZ:** Yo sí voy a hacer uso de mi tiempo, señor presidente, porque antes ha hablado el compareciente de Estados Unidos y quería comentar que en la nueva estrategia de seguridad nacional que el PP ha consensuado con Ciudadanos y el Partido Socialista se incluye la desinformación como una amenaza, y desde el Grupo Parlamentario de Unidos Podemos tenemos miedo de que la aplicación de soluciones por parte del Gobierno desemboque en medidas que vayan a poner en riesgo la libertad de información y la libertad de expresión. Y para hablar de libertad de información creo que hay que hablar de la neutralidad en Internet. En el año 2015 Obama durante su mandato como presidente de Estados Unidos aprobó una normativa por la que se garantizaba el Internet igualitario, es decir, todo el tráfico de datos que transita por la red ha de ser tratado por igual, sin ningún tipo de cobro diferencial al usuario o discriminación. Ha llegado Donald Trump y la FCC, la agencia estatal que regula las telecomunicaciones en Estados Unidos, anunció una propuesta para poner fin a esta normativa, una propuesta que se aprobó el pasado 14 de diciembre y que bajo el nombre Restaurar la libertad en Internet esconde el control de las empresas de telecomunicaciones para gestionar el tráfico de Internet bajo su criterio. Esto se traduce en que las grandes empresas de telecomunicaciones decidirán qué páginas van más rápidas y cuáles menos para los usuarios de manera discrecional. En el siglo pasado una de las grandes preocupaciones para que la libertad de información y de prensa fuera una realidad tenía que ver con las imprentas. Las imprentas del nuevo tiempo son las empresas de telecomunicaciones; la libertad de imprenta antes y la neutralidad de la red ahora, la que acaba de cargarse Donald Trump en Estados Unidos. Y con otro tipo de medidas similares le están siguiendo, entre otros, Alemania, Macron en Francia y, con lo que hemos comentado antes, el Gobierno de Rajoy en España. Y le pregunto al compareciente: ¿Considera que sería una amenaza global para la libertad de información y, sobre todo, para el derecho a la información lo que se ha aprobado en Estados Unidos sobre la neutralidad en Internet? ¿Podría afectar de alguna manera a España?

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Del Olmo.

¿Desea intervenir la señora Botella? **(Denegación).**

Tiene la palabra el señor Cosidó Gutiérrez.

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

Únicamente para hacer mención de una sentencia del Tribunal Europeo de Derechos Humanos, una sentencia muy antigua, del año 1976, en el caso de Handyside contra el Reino Unido, en la que el tribunal dicta que el derecho a la difusión de ideas incluye y abarca no solo a las inofensivas o indiferentes sino también a las que chocan o preocupan, en la medida en que sin tal libertad, pluralismo y tolerancia no hay sociedad democrática y estimando que el límite a la libertad de expresión solo se encuentra en el discurso del odio o de incitación a la violencia. Y la leo, señor presidente, porque al hilo de este debate creo que define muy bien cuál es la posición de mi grupo parlamentario.

Y sin querer, en absoluto, señor presidente, entrar en ninguna polémica, me sorprende por qué algunos grupos cuando hacen denuncias de amenazas a la libertad se refieren siempre a una democracia tan consolidada y tan ejemplar desde que Tocqueville escribiese *La democracia en América* y no hacen referencia a otros muchos países que tienen un déficit democrático tan importante.

Muchas gracias. **(Aplausos).**

cve: DSCG-12-CM-82

El señor **PRESIDENTE:** Tiene la palabra el señor Sánchez.

Las cuestiones de derecho comparado e incluso de derecho constitucional histórico si quiere las contesta y, si no, no.

El señor **SÁNCHEZ ALMEIDA** (Director jurídico y miembro de la junta directiva de la Plataforma en Defensa de la Libertad de Información, PDLI): Gracias.

Sobre lo que preguntaba el señor Del Olmo acerca de si la desinformación es una amenaza o no, ustedes ya tienen tres proposiciones no de ley al respecto sobre las *fake news.* Hay discrepancias entre los diferentes grupos políticos. Pienso que esta es una materia sobre la que sería fundamental que se llegase a un consenso. A pesar de la distancia que separa a los diferentes grupos, entiendo que los desafíos que representa Internet para nuestras democracias se tienen que abordar con talante y consenso, es necesario. Pienso que es un error tratar esta desinformación estableciendo una autoridad que diga lo que es verdad y lo que no es verdad. Lo que es verdad y lo que no es verdad —vuelvo a repetir— lo fijan los jueces; para eso están los jueces. Si alguien considera que una información no es veraz tiene el derecho de rectificación. Si alguien considera que una información es difamatoria, tiene las acciones civiles y penales correspondientes. Considero que el tema de la persecución de la información es muy peligroso. Es mejor llegar a un consenso al respecto y que en última instancia esté la voz del Poder Judicial para poner paz en todo esto.

Sobre la neutralidad de la red, esta cuestión ha sido un caballo de batalla de los movimientos ciberactivistas durante mucho tiempo, y también de todas las empresas de Internet, que quieren competir en igualdad. Básicamente, la neutralidad de la red quiere decir que todos los paquetes de datos fluyan por igual, sin discriminación alguna. Precisamente porque afecta a derechos fundamentales la neutralidad de la red soy optimista al respecto. Igual que sucedió con la Ley de Decencia en las Telecomunicaciones del Gobierno Clinton, que fue tumbada en los tribunales, en cuanto a la normativa liberticida en Estados Unidos existen organizaciones de defensa de derechos humanos muy fuertes que pleitean en tribunales y ganan los casos, y pienso que esto es lo que va a pasar en cuanto a la neutralidad, que, desde luego, entiendo que tenemos que defender con uñas y dientes a nivel europeo.

Sobre lo que me decía el señor Cosidó, estoy de acuerdo con que tiene que haber límites. Están tasados en la Constitución los límites a la libertad de expresión. Cuando hay un exceso, tienen que ser los tribunales. Y el discurso de odio tiene que ser proscrito. Pero recuerden una cosa con respecto al discurso del odio: no busquen en las estepas rusas el odio que está naciendo aquí. Me preocupa mucho más el odio de mi vecino de rellano. El odio de mi vecino de Twitter me preocupa mucho más que todas las conspiraciones de *hackers* rusos. Y eso es lo que tenemos que atajar. Es básico preservar el valor fundamental de una democracia que supone la convivencia. Y pienso que tiene que haber un acuerdo entre todos los grupos para impulsar esto.

Muchas gracias a esta Comisión por invitarme. Muchas gracias al Grupo Parlamentario de Unidos Podemos por proponerme. Estoy a su disposición para lo que necesiten.

El señor **PRESIDENTE:** muchísimas gracias a usted.

Compartimos la reflexión final, que el discurso del odio lo tenemos que combatir entre todos y, cuanto más cerca de casa, mejor. **(Pausa).**

— DEL SEÑOR ROMERO BARTOLOMÉ, SOCIO RESPONSABLE DE SOLUCIONES DE SEGURIDAD DE PWC, 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 219/001045 y número de expediente del Senado 715/000357).

El señor **PRESIDENTE:** Vamos a empezar la tercer y última comparecencia de esta mañana. Tenemos entre nosotros a don Jesús Romero Bartolomé, que es socio responsable de Soluciones y Seguridad de PricewaterhouseCoopers. Vamos a intentar que el ponente se ciña a quince minutos, luego habrá un turno de los comparecientes y posteriormente habrá otro segundo turno de preguntas.

El señor **ROMERO BARTOLOMÉ** (Socio responsable de soluciones de seguridad de PwC): Muchas gracias.

Antes de nada quiero agradecer el interés de la Comisión por mi comparecencia, es un placer estar aquí hoy con ustedes para hablar de nuestra visión sobre el estado de la ciberseguridad en España. A la

cve: DSCG-12-CM-82

hora de plantear estos quince minutos de intervención, no he querido caer en lugares comunes, porque seguramente ya habrán tenido otros comparecientes la oportunidad de explicarles la importancia de la ciberseguridad en términos de protección en el ámbito digital de los ciudadanos, en el ámbito de la ciberguerra o ciberdefensa, o en general mirando más hacia dentro a las administraciones, en términos de protección de los activos de información y de los sistemas de información de las propias administraciones y, en definitiva, como habilitador del escenario digital, del negocio o de la sociedad de la información. En el turno de preguntas si quieren comento más temas de contextos, de motivación o ámbito general. Como no puede ser de otra forma, estoy a su total disposición.

Sin embargo, he entendido que podía ser de mayor interés entrar en temas concretos sobre qué preocupa de manera general en nuestros país y a nivel internacional a las empresas; qué oportunidades tenemos encima de la mesa en el ámbito de las iniciativas legislativas en nuestro país; qué relación de aspectos hay entre la posición de ciberseguridad de España con otros países vecinos y a qué es debido; finalmente, daré una breve pincelada sobre la situación de la AGE en términos de ciberseguridad. **(Apoya su intervención con una presentación en Power Point).** Tampoco he querido caer en algo de lo que adolecemos comúnmente las empresas privadas, que es meter unas transparencias sobre lo estupendos que somos y lo bien que hacemos las cosas. Simplemente, quiero hacer unos breves comentarios. Conocerán a PricewaterhouseCoopers, ya que en estos momentos es la principal auditoría financiera y de cuentas del país. En el ámbito concreto de la ciberseguridad somos la principal consultora y auditora y en el ámbito de las administraciones estamos con la práctica totalidad de las comunidades autónomas y prestamos servicios en la práctica totalidad de la Administración General del Estado.

Entrando ya en el tema que preocupa, he elegido un matiz de una encuesta que realizamos anualmente a más de cuatro mil empresas a nivel internacional y a casi cuatrocientas empresas, trescientas ochenta y algo, en el ámbito español. Tienen un enlace en la presentación para profundizar en la información, pero si tienen más interés estoy a su total disposición para pasarles más detalles, o incluso si tienen alguna pregunta o ángulo especial, ya que tenemos toda la información y podemos explotarla. En la pregunta que he elegido tienen el porcentaje a nivel internacional *versus* el porcentaje de los entrevistados españoles. Se les preguntaba qué les preocupaba en términos de ciberseguridad en las empresas públicas y privadas, desde los incidentes que han podido tener hasta su concienciación y posición tecnológica, qué impactos tenían. No hay nada que no sorprenda, desde interrupción de la continuidad de su negocio de las operaciones hasta la pérdida de la información confidencial de los clientes de esas empresas públicas o privadas, o la pérdida de los propios datos de la empresa. Prácticamente uno de cada dos entrevistados en España tenían esa preocupación. Llama la atención que hay un 22 % a nivel internacional y un 25 % en nuestro país que temen el daño a la vida humana y esto lógicamente es otra dimensión respecto a daños económicos o de operación más o menos importantes. Esto es cierto y también les habrán hablado de ello en los sistemas de control industrial, en los sistemas de control de tráfico, semafóricos, centrales nucleares y demás. Es un campo que protegemos en nuestro país desde el Centro Nacional de Protección de Infraestructuras Críticas, de manera acorde a la Ley de Protección de Infraestructuras, que es una de las leyes que tenemos en el ámbito de la seguridad. Hay otras como el esquema nacional de seguridad que aplica las administraciones o ya lo que se recoge en la siguiente transparencia que tienen ahí: el Reglamento general de protección de datos relativamente reciente que entrará en vigor en mayo de este año y que traspone el correspondiente europeo, que ha sido un paso importante para actualizar la LOPD —que era una buena norma en su día— a la realidad que tenemos actualmente.

Quiero destacar en la presentación que tenemos encima de la mesa dos posibilidades de hacer las cosas bien. Por un lado, la Ley de seguridad de redes y sistemas de información, que a su vez traspone la Directiva NIS europea que habla —atendiendo al anteproyecto de ley— de qué medidas y acciones deben tomar ante incidentes y demás, los que llaman los operadores esenciales de servicios en general y también en general los proveedores de servicios digitales. Por otro lado, está el desarrollo reglamentario de la Ley de Seguridad Privada, ya va para cuatro años que se está esperando ese desarrollo reglamentario. Este habla más de las empresas que en general suministramos seguridad.

Digo que son oportunidades importantes porque así como el delegado de protección de datos, esa figura que existe en las empresas en el Reglamento de protección de datos, ha sido un paso importante y es un paso adecuado, quizás tendría más cabida esta medida en el desarrollo reglamentario de la seguridad privada, el establecer que tiene que haber un responsable de ciberseguridad en determinadas empresas y qué perfil ha de tener es un paso terriblemente necesario y el separar —que no es lo mismo—

cve: DSCG-12-CM-82

la seguridad física. A todo el mundo le parecen obvios y necesarios los tornos, los guardas de seguridad, las cámaras, las vallas o la seguridad antiincendio. Sin embargo, toda esta seguridad física no tiene mucho que ver con la seguridad de un sistema de información que necesita perfiles, organizaciones y responsables distintos. Las empresas que prestamos unos u otros servicios también hemos de atenernos a temas distintos, es decir, una empresa que presta servicios de seguridad en la Administración o en las empresas privadas *top* de este país también ha de tener unas características deseadas. Yo creo que estamos —insisto— ante dos iniciativas excelentes, dos oportunidades que no deberíamos dejar pasar porque ayudarán a mantener el nivel de seguridad en este país; nivel que, por desgracia, no es el mismo ahora que hace un tiempo. Hace veinte años éramos un referente en muchos temas. Empezó la Fábrica Nacional de Moneda y Timbre a dar certificados electrónicos en la firma electrónica. Después, empezamos a tributar por Internet, en una iniciativa absolutamente pionera. Todos los países tomaban estas y otras iniciativas nuestras como referencia. Hace diez años lo mismo ocurrió con el DNI electrónico, también fuimos un referente. Sin embargo, a día de hoy no somos precisamente un referente y esto es así debido a un motivo principal, que veremos en la siguiente transparencia.

He elegido dos iniciativas sobre las que no me quiero extender más. He elegido Reino Unido y Francia, como podía haber escogido Alemania o cualquier otro país vecino, con un resultado absolutamente similar. Ahí tenemos dos iniciativas que si miramos nuestra estrategia de ciberseguridad nacional, más o menos, tampoco son temas que nos llamen la atención. Una es el plan quinquenal que lanzó en 2016 nuestro vecino de Reino Unido y otra es la revisión que ha realizado hace poco en 2017 nuestros vecinos franceses. Son iniciativas que si leemos sobre los negocios en la red, sobre la sensibilización, o sobre cualquier otro de los puntos, no nos son ajenas ni extrañas, no hay ningún invento nuevo. Lo que sí es muy diferencial es la dotación presupuestaria. Mientras Reino Unido a ese plan le dedica 2300 millones de euros y Francia le dedica aproximadamente 1000 millones a la iniciativa que ha revisado el año pasado —tienen en el pie de la presentación las fuentes de información—, nosotros le estamos dedicando unos 24 millones de euros al Incibe y unos 160 millones de euros al CCN del Centro Nacional de Inteligencia. Señorías, ustedes sabrán mejor que nadie que las iniciativas que se legislan o que se impulsan, de manera directa o indirecta, si no están dotadas de presupuesto no traccionan. Sobre la base de la crisis, siendo necesario que el Estado dote de presupuestos a otros temas también muy importantes y de mucho interés, este no tiene ni de largo la dotación que requiere y estamos a mucha distancia. Este no es un tema de cuanto más presupuesto mejor en general —aunque si viniera alguien de una empresa diría que quiere más presupuesto porque es parte de la empresa y hay administraciones públicas que son clientes suyos—, sino que es un tema de que la distancia del presupuesto me sitúa al nivel de países que en otros ámbitos no tienen ni por asomo el desarrollo que tiene el nuestro.

En cuanto a la Administración —esto lo conocerán igual o mucho mejor que yo— este es el modelo organizativo que tenemos para la ciberseguridad de nuestro país desde un ámbito más estratégico y político, bajando hacia el plano táctico operativo y en último lugar está el técnico, que son los CERT de Defensa, el de seguridad e industria que explota el Incibe y el de las administraciones públicas que explota el Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia.

Volvemos a lo mismo. Tenemos excelentes profesionales en la Administración —por supuesto también en las empresas a una de las cuales represento hoy aquí—, pero lo que faltan son medios. Tenemos profesionales en estas distintas entidades que están sacando un euro y medio o dos euros, cada euro de presupuesto que se les da, pero realmente al nivel que pueden llegar con la dotación que tienen es el que es. Por poner un ejemplo, se anunció a finales del año pasado un centro operativo de seguridad que iba a subir sensiblemente el nivel de base de la seguridad de las administraciones. Fue anunciado, pero parece ser que a día de hoy está parado el tema por un tema exclusivamente presupuestario. Al final, siendo necesarias distintas inversiones en valor absoluto en euros, las inversiones en ciberseguridad son mucho menores que otras posibles inversiones en el ámbito de las Fuerzas y Cuerpos de Seguridad del Estado, o en el ámbito general de la Administración General del Estado.

Aquí tenemos algunos de los retos actuales de las propias administraciones. Ahora me centro ya en mirar las administraciones y sus estados, es decir, en cómo están los sistemas de información de los distintos organismos e instituciones de la Administración General del Estado. Podríamos hablar lo mismo de la práctica totalidad, con alguna honrosa excepción, de las comunidades autónomas. ¿Cómo tenemos los datos de nuestros ciudadanos o los datos estratégicos para nuestra Administración o nuestro Estado, cómo están de bien protegidos? Existen líneas en los que son bastante mejorables. Ahí hay algunos de los retos y algunas de las tareas pendientes, una vez más debido a un tema absolutamente presupuestario.

cve: DSCG-12-CM-82

Por cierto, son retos y acciones a tomar que por lo demás están perfectamente alineadas con las líneas de actuación que se fijaron en materia de ciberseguridad dentro de nuestro Plan estratégico nacional del año pasado y que tienen también ahí recogidas en la presentación.

No sé si he conseguido el reto de ceñirme a quince minutos.

El señor **PRESIDENTE:** Lo ha hecho usted muy bien.

El señor **ROMERO BARTOLOMÉ** (Socio responsable de soluciones de seguridad de PwC): Quedo ahora a su total disposición.

Como ven he pretendido abrir una serie de temas, que entiendo que son relevantes y de gran interés, de puertas para afuera de nuestras administraciones y de puertas para dentro. Ahora quedo a su total disposición para las preguntas que crean convenientes.

El señor **PRESIDENTE:** Muchísimas gracias. Ya verá usted como los portavoces lo hacen igual de bien que usted.

Por el Grupo Mixto, tiene la palabra el señor Xuclà.

El señor **XUCLÀ I COSTA:** Muchas gracias, señor presidente, por su presunción de bondad con respecto a los portavoces.

El señor **PRESIDENTE:** De eficacia, de eficacia. **(Risas).**

El señor **XUCLÀ I COSTA:** Muchas gracias, don Jesús Romero Bartolomé, por su intervención inicial.

Voy a centrar mi intervención en plantearle básicamente algo que usted ha apuntado, que es mi preocupación por una dimensión muy importante de la ciberseguridad, que es el ciberespionaje en el ámbito de la propiedad intelectual. Evidentemente, existe el ciberespionaje en el ámbito de la inteligencia política, en el ámbito de lo público, pero las empresas están muy preocupadas porque las patentes tienen un valor económico muy importante. Tenemos datos y elementos para considerar que la mayor actividad en el ámbito del ciberespionaje se produce entre particulares, con el objeto de robar precisamente la propiedad intelectual. En este sentido, me gustaría que desarrollara un poco más al respecto y especialmente cómo se canalizan los litigios en los tribunales para pedir el resarcimiento de los daños causados por el robo de propiedad intelectual en caso de ciberespionaje entre empresas. Como usted conoce esta es una realidad muy compleja pero muy importante, ya que las empresas españolas están siendo hackeadas básicamente para intentar robar su creación, que es la propiedad intelectual.

Termino con dos aspectos, brevemente. Usted nos ha hablado de algunos buenos momentos muy positivos de hace diez años y nos hablaba de la firma electrónica. Yo me acuerdo perfectamente de un caso práctico cuando al inicio de una legislatura en esta casa nos dieron un curso para la firma electrónica, de tal forma que podíamos presentar preguntas parlamentarias con firma electrónica. Le tengo que confesar que nunca operé con la firma electrónica. No estoy ridiculizando este tema, sino que me gustaría conocer la salud de la firma electrónica que gestionaba la Casa de la Moneda y cómo se ha desplegado esta oportunidad.

Finalmente, tomo nota de algo que usted nos ha apuntado que es la deficiente dotación presupuestaria para hacer frente a los retos. Esto lo tendremos que discutir en este Congreso de los Diputados el día que haya un proyecto de Presupuestos Generales del Estado. Después veremos las partidas presupuestarias y consideraremos si el Gobierno ha sido sensible a la necesidad del incremento de las mismas.

Muchas gracias.

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

Por el Partido Nacionalista Vasco, señor Legarda.

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

Muchas gracias, señor Romero, por las explicaciones que nos ha dado. Yo seré muy breve. Me gustaría preguntarle su opinión sobre tres aspectos. Me ha dado la sensación, por su intervención, de que ha concebido las cuestiones atinentes a la ciberseguridad de una manera jerárquica, es decir, la Administración como elemento tractor. Sin embargo, parece que hay un consenso que es una misión de todos los agentes y singularmente esta colaboración público privada, a su vez también de la educación a

cve: DSCG-12-CM-82

todos los niveles y de los alineamientos internacionales de las alianzas. Me gustaría, si pudiera, que nos comentara alguna cuestión relativa a estos tres aspectos porque me parece que se ha centrado mucho, o igual ha sido su intención, en la parte pública. Son esos tres temas: la colaboración público privada, las alianzas y la educación.

El señor **PRESIDENTE:** Por el Grupo Ciudadanos, señor Gutiérrez.

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

Muchas gracias, señor Romero Bartolomé, por su exposición y por su comparecencia que le agradecemos todos en el día de hoy. Aunque tengo un par de preguntas que hacerle, quisiera mostrarle mi extrañeza por que en la diapositiva en la que presentaba las amenazas, tal como las veía, en las empresas no estaba recogido el daño reputacional. Estoy seguro de que en algún sitio debe de estar porque hoy en día uno de los actos más sencillos y más frecuentes, para las propias empresas y la propia Administración e incluso para los propios ciudadanos, es destrozar la reputación de empresas y personas, precisamente a través no solo de estas noticias falsa de las que venimos hablando durante todo el día de hoy, sino también mediante ataques directos que en el caso de competencia yo sé que se realizan. Hay una parte que no ha mencionado que es cómo se está usando dentro de la industria precisamente este tipo de técnicas de atacar la reputación de otras empresas por parte de otras empresas. Dentro de la competencia desleal, aparte del delito que pudiera suponer, esto se está utilizando. Esto es algo que no se suele mencionar, cómo unas empresas están empezando a utilizar este tipo de técnicas para atacar a la competencia. Esto es algo que también es importante aunque no está regulado de forma clara y no se trata tampoco en los tribunales de la defensa de la competencia. No se está haciendo mucho sobre esto y me gustaría poner foco en este asunto.

Yo no estoy muy seguro de que el Reglamento de seguridad privada, que afecta exclusivamente a las empresas de seguridad privada y que están claramente determinadas por su objeto social, tenga mucho que ver probablemente en esto, entre otras cosas, porque cada empresa debe tener la posibilidad de organizarse y allá los clientes que contraten con ellos. Yo creo que entra dentro de cómo se debe de competir dentro del mercado. Nuestro grupo parlamentario no es particularmente muy intervencionista en este tipo de cosas y nos gustaría que nos aclarara, al igual he entendido mal, si usted piensa que debería crearse un figura al respecto. Yo no lo he entendido muy bien; no he entendido muy bien qué pintaba aquí el Reglamento de seguridad privada dentro de lo que estábamos hablando.

Es evidente que la dotación presupuestaria es algo esencial dentro de la Administración y también la partida que dedican las empresas a su propia seguridad. En ese sentido está la libre competencia y qué empresas son más seguras y menos seguras, hablamos de sus clientes y proveedores. En cuanto a los Presupuestos Generales del Estado para 2018 —espero que al final este Gobierno los traiga aquí—, creemos que estas partidas deben incrementarse notablemente. Efectivamente, la Administración adolece ya no solo desde el punto de vista de la propia infraestructura de la Administración, sino de la propia generación de la cultura de seguridad y es algo que sin presupuesto es imposible hacer. Yo creo que hay muchísimo voluntarismo, pero poco presupuesto. Me gustaría que nos comentara un poco qué idea tiene usted, de qué fórmula podría utilizarse para mejorar esta cooperación público privada. Más allá de la protección a las infraestructuras críticas, cuestión que está absolutamente clara, creo que hay otros mecanismos —mi grupo lo entiende así, pero nos gustaría saber su opinión— para mejorar estas fórmulas.

También me gustaría hacerle otra pregunta. Ha costado muchísimos años a la Administración española tener un CIO, Chief Information Officer, un director, así como servicios de información para la Administración. No sé si coincidirá conmigo en que es necesaria la creación de la figura dentro de la Administración de un CSO, un Chief Security Officer, que al final sea el responsable de la implantación dentro de nuestra Administración de estos sistemas de seguridad. Mientras no exista y se consolide un responsable de la seguridad de toda nuestra Administración, si es algo que dejamos en función de cada ministerio, yo creo que probablemente no conseguiremos nunca tener una política de seguridad —estoy hablando solo de la Administración— de la Administración eficaz, ni una cabeza visible que sea capaz también de impulsar un presupuesto adecuado para esto.

Muchas gracias.

cve: DSCG-12-CM-82

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

Probablemente la experiencia israelí nos pueda servir de referencia porque acaban de unificar todos los servicios en una oficina que depende del primer ministro. Buscaremos, si les parece, documentación y la iremos repartiendo entre los senadores y diputados.

Por el Grupo de Unidos Podemos, tiene la palabra el senador Comorera.

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

Muchas gracias, señor Romero, por su comparecencia en el día de hoy. Me gustaría saber, en primer lugar, de qué manera considera que se debería abordar desde la Administración la creciente expansión del llamado Internet de las cosas, tanto desde el punto de vista de la Administración como desde el punto de vista de la seguridad privada. Estamos completamente de acuerdo con usted en que hay una falta de inversión en ciberseguridad. No hace mucho don Enrique Cubeiro, jefe de Operaciones del Mando Conjunto de Ciberdefensa, manifestó que se invierte más en vallas, que en ciberseguridad y se pregunta que de dónde vendría el siguiente ataque, si vendría a través de una valla o a través de un Firewall. Estoy completamente de acuerdo con lo que ha manifestado sobre el problema grave que existe de falta de inversión en ciberseguridad. Además, dejo caer la pregunta: ¿no debería aprovecharse invertir mucho más como una oportunidad de crear empleo y desarrollo? Por esa vía podríamos conseguir muchos nuevos puestos de trabajo.

Precisamente uno de los objetivos de la Estrategia de Seguridad Nacional es favorecer la innovación en seguridad y apostar por la tecnología y la I+D+i española. Nosotros nos felicitamos por ello, pero creemos que a día de hoy el desarrollo de la I+D+i está a unos niveles ínfimos, pues los datos no hacen más que confirmar que la inversión sigue perdiendo peso, pese a la recuperación económica de las cifras macro. Me gustaría conocer su opinión no solo con relación a ciberseguridad sino en inversión en I+D+i.

Otro de los objetivos de la Estrategia de Seguridad Nacional es avanzar en el cumplimiento de la normativa sobre protección de infraestructuras críticas en el proceso de planificación escalonado previsto en dicha normativa. Como profesional experto en seguridad TIC, ¿cómo valoraría el estado actual de cumplimiento de la normativa por parte de las infraestructuras?

Otro dato preocupante que fue publicado hace unos días es que el 49 % de las empresas españolas no tiene una estrategia integral de ciberseguridad. ¿Qué se debería hacer desde la Administración para intentar cambiar esta tendencia?

Por último, he visto en su excelente currículum que usted trabajó ocho años en Indra, que fue una de las empresas que participó en el desarrollo de LexNET. Si bien parece ser que no trabajaron en el dimensionamiento inicial de la plataforma ni en su desarrollo, mantenimiento y resolución posterior de incidencias, me consta que han prestado servicios de coordinación en la adaptación y la implantación en determinadas comunidades autónomas o ciudades de todos los proyectos o sistemas del Ministerio de Justicia. No sé si usted ha participado personalmente en ello de alguna forma, pero, en todo caso, me gustaría que me diera su opinión sobre la crisis de LexNET o sobre los problemas de ciberseguridad que podrían existir en la denominada justicia digital.

Muchas gracias.

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

A continuación, por el Grupo Socialista, tiene la palabra el señor Cortés.

El señor **CORTÉS LASTRA:** Gracias, señor Romero, por su intervención porque nos ha aclarado algunos asuntos.

Yo hacía una cierta similitud entre su intervención y la intervención del primer compareciente de hoy. Es cierto que quizás aquí en esta Cámara tenemos la obligación de gestionar con responsabilidad el presente, pero también tenemos la obligación de tratar de imaginarnos un poco el futuro, hacia dónde vamos. Quizás en este asunto no estamos en el camino adecuado. Cuando hablaba del presupuesto que dedica Reino Unido o Francia y el presupuesto que estamos dedicando en España, rápidamente he hecho una multiplicación. Me he imaginado, manteniendo este mismo presupuesto durante cinco años, en qué niveles podemos encontrarnos y España se puede encontrar en torno a los 630 millones de euros y Reino Unido se encontraría en 11 500 millones de euros. Difícilmente podríamos recuperar ese terreno con celeridad y estar en una situación de igualdad, o al menos de seguridad hacia nuestros ciudadanos, hacia nuestra Administración pública y hacia nuestras empresas privadas.

cve: DSCG-12-CM-82

En todo el diseño que ha realizado en su intervención me gustaría ceñirlo a tres cuestiones muy básicas. En primer lugar, están las empresas privadas. Usted hablaba de responsables de ciberseguridad, que en el futuro deberían formar parte de una manera estable en la organización de esas empresas privadas. En segundo lugar, hemos hablado con el primer compareciente —en este sentido sería interesante conocer su opinión— sobre los certificados de ciberseguridad. Y en tercer lugar, hablamos mucho de la cultura de defensa en la Comisión de Defensa, de la cual formo parte, porque sabemos que tenemos un déficit en este país de la cultura de la defensa.

Ahora que el presidente hablaba de la cultura de la seguridad, quizás también debamos empezar a hablar de la cultura de la ciberseguridad. Deberíamos hablar de la cultura de la ciberseguridad desde el inicio, desde la educación, como hemos comentado en esta Comisión. Por un lado, hay empresas privadas, y por otro, está la organización de la esfera pública. También quiero conocer su opinión —el primer compareciente nos hablaba de ello— sobre un liderazgo único. Ahora el presidente hacía mención de lo mismo, ver cómo se puede organizar la Administración desde lo público para dar una vertebración mejor a la colaboración público privada en este ámbito de la ciberseguridad y un compromiso en el ámbito presupuestario para no perder tiempo porque aquí estamos perdiendo el tiempo; estamos perdiendo el tiempo en materia de ciberseguridad.

Termino, presidente. En este país está ocurriendo un enorme desajuste entre la inversión que están dedicando las grandes empresas de manera inteligente —hablo del Banco Santander, BBVA o Telefónica— en materia de ciberseguridad y lo que estamos dedicando desde la Administración. Por tanto, si nosotros dedicamos menos recursos y al mismo tiempo estamos hablando de una colaboración público privada ¿de qué manera podemos hacerla en el futuro, si no estamos ni siquiera en una situación de igualdad? ¿No tendríamos que activarla? ¿Cuál es su opinión? Sé que ya se lo han preguntado dos de mis colegas, pero quiero preguntarle también sobre este asunto: el asunto de la colaboración público privada.

Termino con una última cuestión, presidente, si me lo permite. ¿Dónde debe priorizarse en la Administración? Me gustaría que nos dijera las dos o tres medidas que usted considera que la Administración pública debería priorizar en materia de ciberseguridad.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias a usted, señor Cortés.

El señor Mateu Istúriz tiene la palabra.

El señor **MATEU ISTÚRIZ:** Señor presidente, buenos días y muchas gracias.

Es la primera vez que intervengo en esta Comisión y desde luego es muy interesante y agradezco enormemente a mis portavoces, tanto del Congreso, la señora Vázquez, como el portavoz en el Senado, señor Aznar, que me permitan intervenir en esta ocasión, porque desde luego el tema bien merece la pena.

Señorías, en definitiva, la presencia del señor Romero ha sido muy ilustrativa en algunos temas en los cuales él ha entrado en gran profundidad. Su presencia aquí es un aval. ¿Por qué? Por su propia preparación. Ser ingeniero de telecomunicaciones, luego haber hecho un MDA y tener una certificación que va a entrar dentro de lo que es la pregunta que le voy a hacer a usted. El Thirty Five Information Security Manager es un marchamo y un aval de calidad, sobre todo en el ámbito en el que usted se mueve, que es una empresa como PricewaterhouseCoopers que evidentemente es tan alta su digitalización, tan alta su tecnificación, que ustedes son sujetos pasivos de los ciberataques y sujetos activos para entrar en la defensa de los mismos. Es una realidad, la que todos hemos hablado, todos los grupos parlamentarios aquí, de que el ciberataque existe. No solamente existe en el seno de las empresas privadas, como usted representa, y existe en el ámbito del día a día y fundamentalmente es un grave peligro para lo que es la cotidianeidad del día a día de la garantía de vida y tranquilidad de vida de los propios ciudadanos. Tenemos claros ejemplos. Inmersiones en procesos electorales, inmersiones en robo de datos de empresas o de destrucción masiva o de suplantación de identidad. Aparte de la ciberseguridad es un momento de plantearle como pregunta diferencias, peligrosidad, riesgos de lo que es los ciberataques con lo que son las *fake news*. Noticias falsas, rumores, que también hacen mucho daño en procesos productivos y también en generar una opinión en la ciudadanía. Por eso quiero saber qué peligros detecta usted en cada una de ellas, aunque son comunes en lo que probablemente algún tratadista ha llamado lo que es la guerra híbrida.

Quiero recordarles lo que está sucediendo en estos momentos con la tecnificación y que no podemos prescindir de aparatos conectados a Internet y a las redes sociales, como puede ser —y

cve: DSCG-12-CM-82

recuerdo las palabras del general Gómez López de Medina, jefe del mando conjunto de ciberdefensa en esta Comisión el pasado 27 de noviembre de 2017— el ciberespacio lo inunda todo, desde que llevamos un *smartphone* encima nuestra vida está más en el ciberespacio que en la realidad, nos despierta por la mañana y nos conduce a lo largo de toda la jornada y además, usted lo ha mencionado, el entorno legal es muy complicado. Este es el punto de partida básico de lo que verdaderamente le preocupa al ciudadano y una vez que tengamos al ciudadano convencido de lo que está haciendo su ser supremo, que es el Estado, que son las empresas que tienen que colaborar, entonces la vida será mucho más sencilla para todo el mundo. Se dice que un ciberataque se lleva más tiempo en la preparación que en la propia ejecución.

Otra pregunta: ¿Por qué no ponemos los mecanismos necesarios para abortar ese plan de ataque antes de que el mismo se ejecute? También se dice, señor Romero, que es más barato atacar que defender. Pongamos los medios para que esto no sea así una realidad. Usted hablaba de una escasez de presupuesto. También le voy a preguntar qué conceptos o tributarios o de tasas podría usted obtener de un Estado ahora mismo de ingresos en unos Presupuestos Generales del Estado para reforzar lo que ahora califica de una baja dotación presupuestaria.

Otra pregunta que le voy a hacer, porque aquí hay temas comunes que hay que repetirlos, independientemente de que otros compañeros de otros grupos lo hayan preguntado en esta Comisión. ¿Qué papel jugaban ustedes en la ciberseguridad? ¿Qué colaboración público-privada se puede establecer con el Estado para que todos trabajemos al unísono? ¿Qué papel tienen que jugar las universidades? Porque se ha hablado de la enseñanza a niveles inferiores y de la Formación Profesional. Las universidades se dedican ahora mismo a los *papers* promoción interna de los profesores o están cumpliendo el papel que realmente tienen que hacer sobre la investigación para crear el talento necesario para tener a gente formada en estos temas. Coordinación, usted nos ha puesto de manifiesto esos entes administrativos, que hay varios. ¿Qué podemos hacer? ¿Estamos seguros con la coordinación que hay actualmente o cree que es perfectible como toda empresa humana? Yo le digo que el Gobierno del Partido Popular está empleado a fondo en garantizar la ciberseguridad y creo que funciona prácticamente como un reloj suizo todos los engranajes de comunicación y de mecanismo que existe en la comunicación, por ejemplo, de los episodios de ciberataques.

Un tema importante que a usted le afecta como partícipe de una gran empresa. ¿Puede ser la ciberseguridad una opción para nuestro desarrollo industrial, económico y social? Entiendo que sí, por supuesto, pero quiero saber también su opinión.

Hemos hablado de educación —antes hablaba un compareciente que me ha parecido muy bien, porque yo he participado en temas de calidad también y he participado en poner en marcha sistemas de gestión tributaria automatizados, como se llamaban en un momento determinado—, antes hablábamos de calidad y este ponente anterior, el primero, decía que ahora la calidad está incorporada en todos los procesos productivos, ahora hace falta incorporar la seguridad y eso es tarea de una colaboración público-privada.

Por último, para no agotar la paciencia del señor presidente y de los miembros de la Comisión, me remito al informe que su empresa elaboró, que me ha parecido muy interesante, la encuesta mundial sobre el Estado de seguridad de la información de 2018. El compañero ha incidido qué pocos son los empresarios que dicen que tienen un plan de ciberseguridad de ataques en su propia empresa, un 49 %, cuando realmente afecta a pérdida de datos sensibles, alteraciones del activo, falta de confianza en los procesos productivos, falta de calidad y eso es un tema que también hay que pelearlo para sacarlo adelante.

Una pregunta, que desde luego el Partido Popular está muy interesado, que es la ciberreserva, tener un complejo de personas, hombres, mujeres, en España, preparados para en un momento determinado entrar en acción a requerimiento de la autoridad cuando se produzcan ciberataques masivos como ha sucedido recientemente. Si es necesario tenerlos preparados en cualquier momento, como los reservistas del Ejército, y una coordinación hacia ellos. Nosotros entendemos que es muy importante que exista un complejo de personas dedicados a esos menesteres, que colaboren de una manera altruista, de distintos orígenes o procedencias con el tema de los ciberataques en estos momentos.

Señor presidente, muchas gracias, y espero su contestación, señor Romero, y muchísimas gracias por su presencia.

cve: DSCG-12-CM-82

El señor **PRESIDENTE:** Muchas gracias, señor Mateu Istúriz.

Aprovecho para darle la bienvenida a esta Comisión. Tiene la palabra el compareciente. Le vamos a conceder diez minutos también.

El señor **ROMERO BARTOLOMÉ** (Socio responsable de soluciones de seguridad de PwC): No sé yo. Haremos lo posible porque son muchas las preguntas, muy interesantes y la práctica totalidad muy bien traídas.

Empiezo por el final. Creo haber tomado buena nota, a su disposición en segunda ronda si algún tema o alguna pregunta omito. El tema de la ciberreserva. Es un tema complicado. Es un tema que más allá de estar a favor o en contra, yo le veo una dificultad operativa. Es un tema terriblemente emergente que todavía no ha aterrizado, pero hay una dificultad operativa de cómo se moviliza la ciberreserva, de los ciberreservistas que estarán trabajando como responsables de seguridad en el ámbito público o en empresas privadas, más allá de la buena voluntad, cómo se moviliza esta gente si están atendiendo a un incidente de un banco, porque trabajan en ese banco, o de otro ámbito. Además la diferencia que hay con los reservistas del Ejército que ha tenido una instrucción, una formación, y pasa a la reserva. Que una persona que esté trabajando en ciberdefensa pase a la ciberreserva es bastante obvio e inmediato porque conoce la propia operativa, pero es extremadamente difícil coger una persona el de más conocimientos y meterle de forma operativa que defienda un ataque además teniendo en cuenta lo que ha comentado, que es verdaderamente cierto, que es la inmediatez en el tiempo del ataque. Ahí más que entrar en consideraciones políticas, que las hay en el debate político, le veo un tema operativo a tener en cuenta.

Yendo por el orden de las preguntas, en cuanto al tema de los litigios y, en particular, en el ciberespionaje y en la propiedad intelectual. Qué duda cabe que cuando hablamos de proteger los activos de información de las empresas, el tema de patentes es un tema fundamental igual o más importante que sus datos estratégicos, de planes estratégicos o de expansión internacional, por ejemplo. Hay sectores como el sector de la tecnología o el farmacéutico donde es fundamental esa protección. Las empresas se debaten en dos opciones a la hora de tener un ciberincidente que es en mayor o menor duda hacerlo público o comunicarlo empezando por las propias Fuerzas y Cuerpos de Seguridad del Estado o el mantenerlo confidencial entendiendo en una visión, desde mi punto de vista equivocada, que con el secretismo, la no colaboración, intentando que no salga fuera, puede ser más beneficioso para la empresa en términos de reputación. Esto se normalizará, que las empresas han de normalizar, el Reglamento de Protección de Datos ya obliga a ello a que los incidentes se comuniquen. La trasposición de la Directiva NIS, la Ley de seguridad en redes y sistemas también obliga a ello y es un tema importante.

En cuanto a los litigios realmente son complicados. La legislación que tenemos es la que es y en el ámbito transnacional es la que es. Los litigios son complicados. La custodia de la cadena de evidencias es complicada de por sí, porque tenemos unas leyes que tradicionalmente vienen del ámbito físico, por decirlo así, y hay que aplicarlas en el ámbito digital. En estos temas y especialmente a la hora de informar a quien proceda de los ciberincidentes ahí tienen ustedes todos los grados de libertad para acabar de aterrizar la ley que traspone la Directiva NIS y eso es un ámbito de mucho interés. Las empresas, desde mi punto de vista, han de verse obligadas a publicar los incidentes y, una vez que sea así, vendrá ya corrido, por supuesto, la denuncia, una vez que estén obligadas a reportar de forma natural denunciarán y pondremos en marcha el mecanismo con todas las limitaciones o grados de libertad que nos permita el marco normativo vigente que, como todo en la vida, es susceptible de evolución y de mejora. En cuanto a la salud de la firma electrónica está muy sana. En la experiencia que ha comentado su señoría sobre Indra, tuve la ocasión no solo de estar bajo mi dirección el despliegue del DNI electrónico y la firma digital en CD, sino la propia iniciativa del Congreso de portafirmas y de dotar a sus señorías de firma electrónica. Lo conozco bien. Está sana, está vigente. Tiene una solidez en virtud de la normativa vigente es equiparable a la manuscrita con toda la solidez jurídica y hay iniciativas como siempre se puede sacar mayor provecho, se pueden hacer más iniciativas y podemos usar más el DNI o la firma electrónica de CD o de cualquier otro prestador de servicio reconocido o certificación, que es el término que establece la Ley de Firma Electrónica. Diría que está sana aunque en el horizonte, ya si nos metemos en el tema tecnológico me tengo que medir, porque sobrepasaría con mucho el tiempo que me ha dado el señor presidente, tenemos iniciativas como el *blockchain,* que están llamadas a cambiar, no el panorama de la firma electrónica, muchos, muchos procesos administrativos y de negocios en las empresas y es una tecnología emergente pero sobre la que oiremos hablar mucho, se sale del ámbito de mi intervención, pero es un tema que da para hablar toda una mañana.

cve: DSCG-12-CM-82

Respecto a la parte internacional de colaboración, de alianzas y demás, qué duda cabe, he enfocado mi intervención inicial hablando de que puede ser de interés para las Cámaras y en general para la Administración mirando hacia fuera a los administrados y a las empresas y mirando hacia dentro. No quería hacer una taxonomía completa, pero es un tema internacional, de colaboración, de seguridad concertada, cada vez más los ciberataques y los ciberdelitos son transnacionales. Por supuesto, está el tema que ha salido en dos o tres preguntas de la colaboración público-privada. La colaboración público-privada esta ahí y creo que la parte privada está interesada, está capacitada y puede estar interesada en el tema. Puede ser no la única, pero una palanca importante, junto con más dotación presupuestaria, sin la cual difícilmente se puede sacar más jugo del que están sacando ahora los excelentes profesionales de los distintos organismos o instituciones de las distintas administraciones. La colaboración público-privada está ahí y los modelos hay que estudiarlos. Hay que estudiar los modelos en un tema que es de la seguridad y, en particular, de la ciberseguridad, por ejemplo, centros de operación y centros de respuesta puedan estar gestionados de una y otra forma y dentro de los distintos modelos de colaboración público-privada por el ámbito privado puede ser factible pero requiere un estudio de idoneidad, de conveniencia, detallado. En general, estoy de acuerdo en que la colaboración público-privada es una palanca a considerar si queremos volver a alcanzar, ya no ser una referencia, como hace diez años o veinte, sino alcanzar el nivel de nuestros vecinos.

En cuanto a los temas que hemos comentado, ataques de reputación que lo ligaría con el tema de *fake news* y demás, en esta parte yo haría una distinción importante. Los temas de *fake news,* los delitos cometidos en el ámbito digital, como la pornografía infantil, como puede ser un fraude, un tocomocho que te hagan en el entorno digital, o un blanqueo de capitales en el entorno digital son delitos cometidos en ese entorno, pero no entran dentro de lo que entendemos por ciberseguridad. Cuando alguien va a una institución o a una entidad hospitalaria público-privada roba datos y luego los vende. Hay dos partes, la parte de ciberseguridad, que roba los datos, y la parte que los vende. Que si los vende impresos en papel será en el mundo físico y si los vende en formato digital en la *deep web*. Pero esa segunda parte tampoco es ciberseguridad. Otra cosa es que sea objeto de estudio de interés de esta Comisión o en general, pero claro que tenemos que preocuparnos por los delitos electrónicos. Es un tema de contenido que puede ocupar y preocupar incluso más alguno que la ciberseguridad. Pero por ciberseguridad entendemos todo lo que tiene de riesgos tecnológicos, ciberamenazas y sus impactos.

En ese sentido, y al hilo de lo que decía el anterior compareciente, yo me preocupo del vecino si tiene animadversión o malas intenciones, pero también me ocupo del que vive en el bloque de enfrente. No solo me preocupo del vecino, sino que sabemos que hay países concretos, hay evidencias, que están algunos con un interés más de desestabilizar y otros con un interés de ir a secretos industriales o de simplemente saber nuestras empresas cuando licitan un tramo de AVE nuevo en un país un consorcio nuestro con qué características, con qué valores añadidos en el concurso y a qué precio van a licitar. Esto existe, sale del ámbito de la ciberseguridad siempre que no haya habido un ataque para acceder a esa información. Obviamente cuando atacan los sistemas y entran dentro y de manera ilícita cogen la información es cuando entra en el ámbito de la ciberseguridad.

Rápidamente. El tema sobre la legislación, que he comentado, y sobre la figura del CISO. No me he debido explicar bien. Me refería en la ley que traspone la Directiva NIS, igual que el Reglamento de Protección de Datos establece que tienen que tener un delegado de tratamiento de datos y eso ha servido a nivel organizativo, de concienciación y ha sido un elemento tractor importante, además de ser, desde mi punto de vista, técnicamente necesario. La Ley de seguridad en redes y sistemas debería establecer que las empresas, para la gobernanza de la ciberseguridad a nivel interno, deberían tener una figura, decir qué perfil y demás. Cuando mencionaba la ley de seguridad privada era a colación de algunas corrientes de opinión, iniciativas, filtraciones, el reglamento tiene una historia larga y ha pasado por distintos estadios entendía que era absorbible las obligaciones, perfiles que se definen, que en este caso para las empresas que prestamos tecnologías o servicios equipararlas de ciberseguridad. Quería transmitirles que si no entran ahí y se siguen basando en seguridad privada el reglamento estará bien, pero en el caso de que se amplíe el reglamento como en algún momento desde alguna corriente de opinión se entendía idóneo o conveniente, en el caso de que se amplíe hay que diferenciar claramente que son colectivos distintos, perfiles distintos y que sería un error intentar con una norma muy enfocada a la seguridad clásica, seguridad privada y demás intentar establecer cuál es el perfil idóneo de empresa de ciberseguridad. Dicho lo cual, y también lo comentaba de pasada, entiendo que podría ser necesario establecer qué requisitos de distinta índole ha de tener una empresa para trabajar en la ciberseguridad de las principales

cve: DSCG-12-CM-82

empresas o en la Administración de nuestro país. Entiendo que puede ser necesario incluso en el tratamiento de determinado tipo de incidentes, de información y demás, sin entrar en más detalle, porque esto abre otro melón importante. Ese responsable que podía recogerse en la Ley de redes y sistemas, en el caso interno de la Administración sería el CISO de la Administración General del Estado.

Aquí hay dos posibles figuras y recojo también otras dos o tres preguntas. Puertas para adentro, para sistemas de la Administración y la información de la Administración podría ser interesante igual que tenemos un CIO de la AGE tener dependiendo de él un CISO de la AGE. Este velaría por los sistemas de la Administración General del Estado y por sus datos. Es una figura que no existe. Ahora, yendo a otras preguntas, este no sería el que otros países han llamado Ciber zar, los estadounidenses y los anglosajones le llaman así. Que es la figura por la que hacía mención otras preguntas que sería el responsable con capacidad operativa o no, dejando las competencias en Interior, en Defensa, en Energía como están ahora o asumiéndolas, que ese es otro debate, alguien que coordine, más allá del buen entente que pueda haber en la Comisión Nacional de Ciberseguridad a día de hoy, y tenga una estrategia en su equipo sobre la ciberseguridad en nuestro país. Insisto, desde un punto de vista político estratégico únicamente o no. Una figura con nivel de subsecretario o de secretario de Estado y que típicamente estaría en Presidencia, como comentaba el presidente en el caso del Gobierno de Israel. Otro tema es el debate operativo si se lleva competencias o no. Que haya una cabeza visible de la estrategia de ciberseguridad a nivel político estratégico es opinable. Hay temas técnicos que no lo son, esto es muy opinable. Yo lo veo como positivo y como un elemento más de tracción y de empuje a la cosa.

En la Internet de las cosas, como en casi todo, no nos han hecho caso a los que estamos en el gremio de la seguridad. Los que estamos en el gremio de la seguridad decimos que lo más barato y lo más eficaz y eficiente para la seguridad es contemplarla desde el momento inicial, desde la fase de diseño, como un requisito. No hacer las cosas y luego ver cómo ponemos los parches. No nos han hecho caso, tenemos juguetes conectados a Internet por Wifi con una cámara que si no tenemos cuidado cualquiera puede ver a nuestros niños o nuestra casa. No quiero lanzar un mensaje alarmista. Una vez más no es un problema español. Este es un problema global, con lo cual el Internet de las cosas hay que tenerlo muy en cuenta y, sobre todo, cuando viene emparejado a lo que se llama el OT, más allá de las tecnologías de la información, el IT, el TI, el ITE, de los sistemas industriales, cuando ya la parte más de sensorización del Internet de las cosas al final con mayor capacidad de inteligencia o menos sensorizaciones. Si no están protegidas puede haber problema en el acceso a información confidencial. Podemos cambiar la medición de determinados sensores y es un tema que requiere de trabajo y susceptible a ser regulado. De ahí, yo me quedo mi parte de la pelota, pero les lanzo a ustedes la parte de la suya.

Totalmente de acuerdo que en el ámbito de la ciberseguridad es un ámbito de desarrollo y que puede crear empleo. Tenemos excelentes profesionales en el ámbito privado también y hemos exportado en un análisis de volumen respecto a exportaciones cuando hace diez años éramos absoluta referencia y exportábamos en volumen absoluto en euros no era significativo, porque tampoco hay el mercado de ciberseguridad que hay ahora. Pero es un ámbito que puede crear más empleo y desarrollar. De hecho hay mucha más demanda de profesionales de los que tenemos y esto enlaza con todo lo que se ha preguntado sobre formación. Muy importante las certificaciones para homogeneizar y saber de qué hablamos. Muy importante que las universidades que tienen master superiores como el modelo de Bolonia de ciberseguridad también se normalice el currículo, porque como una universidad saca un master de ciberseguridad y se le llenan dos o tres ediciones, pero los currículos son dispares, con lo cual la parte de la universidad es un debe que tenemos y por supuesto en el I+D+i aquí no hay nada nuevo. El I+D+i ha subido fruto de la crisis, que es lógico y natural, pero ha tenido unos presupuestos menguantes en los últimos años y habrá más, pero es un tema en el que si ponemos un euro en I+D+i en España va a tener un retorno absolutamente brutal. Pero tampoco estoy en disposición de evaluar si es el tema segundo, cuarto o primero de interés, porque no tengo toda la información ni la foto completa del I+D+i.

En cuanto al sector privado es dispar y enlaza con que por qué el 50 % no tiene un plan de seguridad, por la distribución que hay a nivel internacional en nuestro país de la segmentación de las empresas especialmente si vamos a las pymes pequeñas. El 50 % es el número de empresas. La gran empresa de España tiene un nivel de seguridad muy bueno y no tiene nada que envidiar de los anglosajones, aunque Dios me libre, no tengo ningún tipo de problema con los anglosajones, pero típicamente el modelo suele ser UK o Estados Unidos sobre todo por un tema de volumen. Ejemplo, la banca, cuando nuestros grupos bancarios han adquirido bancos fuera tenían peores controles de seguridad, peores arquitecturas y menos nivel de madurez. Es más, la Administración que estaba a muy buen nivel, como decía hace diez años,

cve: DSCG-12-CM-82

ahora está muy lejos de nuestras empresas privadas. Esto contrasta mucho con el nivel de la pyme, si quitamos la pyme grande, en lo que queda todo por hacer. ¿Ahí qué se puede hacer? Está haciendo muy buena labor Incibe, que es la que cubre ese segmento, sacando euro y medio o dos euros de cada euro que se les da, pero una vez más sus presupuestos son los que son.

El tema del LexNET que no voy a eludir. Antes de tener la responsabilidad que tengo en Price, además estuve en IBM en el comité de dirección llevando para cuatro países, uno de ellos Israel, los temas de seguridad de IBM y antes estuve en Indra, una de las mejores épocas y más interesantes de mi carrera profesional, porque fue donde empecé a ser directivo ejecutivo. Llevaba los temas de seguridad. No sé cómo estaba en ese momento Indra involucrado en LexNET, pero el tema del LexNET más allá de la participación concreta de Indra y del resto de empresas, que sinceramente desconozco, no es propio del Ministerio de Justicia. Entra dentro del problema que tenemos que hemos comentado de presupuestos —supongo, no conozco el detalle— dentro de todo lo que es la Administración del Estado. En el caso concreto de Justicia, que tiene el apoyo de una excelente empresa, que no es la mía ni ninguna que yo haya estado en temas de seguridad, estoy convencido que si no han hecho más ha sido por falta de presupuesto. Hablo desde un punto de vista técnico. LexNET, por lo que he leído en los medios, no tengo más información de la que puedan tener ustedes, por lo que les comento, ha sido un tema de desarrollo de la aplicación. Ahí habría que ver también el nivel de la seguridad. Seguramente no se pudo poner —es una especulación— las medidas necesarias de seguridad en ciclo, vida y desarrollo por falta de presupuesto, supongo.

Por lo demás, ahora me dicen si quieren en segunda ronda, pero creo que se han ido cubriendo todos los temas. Una última, qué acciones podríamos priorizar. Desde mi punto de vista he comentado una que estaba anunciada el año pasado que es un centro de operación de seguridad común a toda la Administración General del Estado. Esta iniciativa, ahora mismo parada, es absolutamente fundamental. Se deberían, desde mi punto de vista, hacer, desde el Centro Criptológico Nacional o quien se considere adecuado, un análisis del estado de seguridad de las principales entidades en términos de ministerios o en general institutos u organizaciones, esto es lo que ayudaría a priorizar si hay algún ministerio poniéndolo junto con la criticidad de los activos de información y de los datos. El Centro de Operación de Seguridad daría un nivel de seguridad a todos, pero luego habría que ver quiénes son los que necesitan acciones más urgentes. Esto para conocerlo hay que hacer un análisis, una auditoría y verlo. Espero haber respondido en mayor o menor medida a sus cuestiones.

El señor **PRESIDENTE:** Si no ha respondido, se lo dirán ahora, en el segundo turno.
Tiene la palabra el señor Xuclá.

El señor **XUCLÁ COSTA:** Gracias, señor presidente.

Intervengo muy brevemente para agradecerle al compareciente su muy interesante intervención. Habitualmente, cuando uno le formula preguntas existe ese estímulo de ir a los casos prácticos. Le he formulado una pregunta y usted me ha contestado, pero en el caso de litigios internacionales sobre propiedad intelectual, de manera muy sofisticada ha dicho que la legislación es la que es —parece gallego— y el contexto es el que es. De su respuesta deduzco que debe ser muy difícil llegar a poder pedir responsabilidades y conseguir la rendición de cuentas ante los tribunales en caso de hackeo de la propiedad intelectual o de patentes. Quería profundizar un poco en esto, siendo muy consciente de que cuando alguien quiere conocer los planes de la alta velocidad en Arabia Saudí, esto está más en el campo de la lucha entre empresas que en el de algo que se pueda dilucidar en los tribunales de forma civilizada.

Usted nos ha provocado, porque ha apuntado el *blockchain* y después lo ha dejado. Es un apasionante tema de actualidad sobre el que no sé si en un minuto o en treinta segundos nos puede trasladar su opinión y decirnos hasta qué punto puede impactar en el mundo económico y en el de la transferencia de información.

Muchas gracias.

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

¿Señor Legarda? **(Pausa).** No está.
Tiene la palabra el señor Gutiérrez.

cve: DSCG-12-CM-82

El señor **GUTIÉRREZ VIVAS:** Gracias, señor presidente.
Quiero agradecer al compareciente sus respuestas y decirle que su exposición ha sido magnífica.
Muchas gracias.

El señor **PRESIDENTE:** Gracias, señor Gutiérrez.
Tiene la palabra el señor Comorera.

El señor **COMORERA ESTARELLAS:** Gracias, señor presidente.
Intervengo brevemente para agradecer nuevamente su respuesta a todas nuestras preguntas. Soy jurista y todo esto de LexNET me interesa mucho. Habla de seguridad, y sin querer abrir ese melón que ha dejado entrever, le preguntaría sobre la posible influencia que puede tener en los niveles de seguridad de las llamadas subcontrataciones y lo de las cárnicas. No sé si le suena el término de las cárnicas y todo esto a nivel de ciberseguridad. Me gustaría conocer su opinión sobre si se tendría que regular o permitir menos este tipo de subcontrataciones que al final puede derivar en un problema de seguridad para determinados proyectos o programas.
Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.
Tiene la palabra el señor Cortés.

El señor **CORTÉS LASTRA:** Gracias, señor presidente.
Yo soy de los que siempre ha pensado que no hay mejor marca España que los españoles que residen en el exterior, porque están en muchos ámbitos. Voy a hacer una pregunta muy breve con respecto al retorno —ha hablado de ello— de científicos, de investigadores, de gente vinculada al ámbito de la ciberseguridad, que están trabajando actualmente en empresas relevantes. Al final, hacer un plan de retorno general es muy complicado, pero tendríamos que pensar que hay sectores estratégicos y tenemos que intentar que esa gente vuelva, tener una escala para que esa gente vuelva, y creo que este ámbito es uno de ellos. Me resulta complicado saber cómo podemos hacerles una oferta desde el ámbito público que sea lo suficientemente sugerente como para que puedan venir a trabajar aquí, porque a lo mejor no les resulta atrayente desde el punto de vista económico, aunque desde el punto de vista privado puede que sí. ¿Cómo cree usted, que ha estado en diferentes responsabilidades en diferentes países y puede conocer a algunos de ellos, que podríamos hacer un plan lo suficientemente eficaz para que esa gente, ese conocimiento pudiera retornar a nuestro país por la vía pública o por la vía privada?
Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Cortés.
Tiene la palabra el señor Mateu.

El señor **MATEU ISTÚRIZ:** Gracias, señor presidente.
Quiero agradecer a mi grupo la deferencia que han tenido dejándome participar en esta magnífica Comisión y al presidente su benevolencia y haberme aguantado más de los cinco minutos preceptivos. También quiero felicitar a este ilustre burgalés compareciente, alto representante de PricewaterhouseCooper, por su magnífica intervención y, sobre todo, por esa disponibilidad que ha tenido en la contestación a todas nuestras preguntas.
Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.
Para cerrar el debate, tiene la palabra el compareciente.

El señor **ROMERO BARTOLOMÉ** (Socio responsable de soluciones de seguridad de PwC): Gracias a ustedes. Ha sido un placer estar aquí. Gracias también al señor presidente por la benevolencia que ha tenido conmigo. Seré breve y no tendrá que aplicar esa benevolencia en esta segunda intervención.
No soy jurista, como ya han comentado, sino ingeniero de telecomunicación, y cuando hablo de litigios lo hago desde la experiencia de haber asesorado a algún cliente en la parte más de ciberseguridad. Al final, los criminales van a intentar monetizar su acción lo más rápido posible, exponiéndose a un riesgo lo menor posible. Esto parece de Perogrullo, pero es lo que está basculando del crimen tradicional al cibercrimen. Si yo entro en un sitio, rompo la pared, o lo que sea, me llevo unos activos materiales y me

cve: DSCG-12-CM-82

voy, luego los tengo que poner en el mercado, durante un tiempo tengo un riesgo mayor y además tengo una legislación en ese país que por lo penal me puede caer lo que sea. Cuando esto sucede en el ciberespacio, estoy en un servidor de las islas que sean —no quiero mencionar ninguna en concreto— y son activos digitales, es cuestión de segundos y por la legislación transnacional es todo mucho más complicado de perseguir. Sin ser un experto en todo el tema criminal transnacional, efectivamente los criminales se están yendo allí porque actualmente, en general, las penas son menores. Los criminales se manejan también desde un punto de vista de inversión y rentabilidad. Ellos tienen una capacidad de inversión, en el mal en este caso, si lo meten en blanqueo de capitales, en negocios del narcotráfico, en trata de seres humanos tienen un riesgo y una rentabilidad, y si se ponen a hacer cibercrimen tienen menos riesgo y más rentabilidad. En cuanto nos vamos al ámbito transnacional de ciber, queda mucho por hacer. Es absolutamente necesaria la colaboración internacional, pero trasciende a cualquier país, en particular a las Cámaras de nuestro país, a los que están en la parte legislativa y a los que estamos en la empresa privada.

En cuanto al *blockchain,* les diré que es una tecnología distribuida en la que no hay una autoridad ni un intermediario central en el que tenga que recaer la confianza, es como si fuera un libro de cuentas o un cuaderno de bitácora que puede ver todo el mundo. Esa base de datos está distribuida y no es modificable fácilmente por uno solo según su interés. Todo esto, y con unas tecnologías subyacentes que no son fáciles ni inmediatas, ni siquiera para los que nos hemos dedicado a la tecnología toda la vida, da la base tecnológica para una revolución importante en la que se puede desintermediar e interactuar o transaccionar de forma más directa en las distintas entidades, sean clientes, empresas, ciudadanos o administraciones. Luego tenemos un caso de uso particular de *blockchain* —hay otros muchos—, que son las criptomonedas. Las criptomonedas por sí solas también dan para hablar largo y tendido. Les pondré un ejemplo. Usando tecnología *blockchain* en el ámbito de los seguros, se podría, de forma segura y con solidez jurídica, que al final, más allá de la tecnología por la tecnología, es estrictamente necesaria, contratar un seguro temporal al montarme en un coche de alquiler y descontratarlo cuando bajo; también podría contratar un seguro cuando empiezo un viaje, cuando subo al avión, y cuando lo termino lo anulo. Estoy desintermediando a la agencia de viajes, a la agencia de alquiler, que ya no me vende el seguro, y estoy cambiando procesos de negocio en el sector asegurador, en el sector de entretenimiento y viajes y demás. Otro ejemplo, quizá más claro. Para gestión de impuestos o para gestión de la seguridad en la cadena de suministro de alimentos, de medicamentos, de licor, de tabaco. Vamos al caso de los alimentos. Con *blockchain,* en el mercado de su barrio o distrito un ciudadano puede coger el código de barras de una caja de merluza y de manera segura, sin que le puedan engañar, sabe la lonja de Coruña —vamos a decir que son de Coruña, porque son buenas merluzas— en la que entró la merluza, a qué mayorista fue, cuándo entró en Mercamadrid y cuándo ha llegado. Lo mismo se puede aplicar para una trazabilidad de medicamento, que tiene otras consideraciones. Insisto en que hay miles de aplicaciones, pero estoy comentando algunas a salto de mata. Deben darse cuenta de cómo impacta en el procedimiento administrativo correspondiente o en el proceso de negocio. Puede ser una revolución. Lo he dicho, repito, a salto de mata, pero he querido dar dos pinceladas sobre un tema que puede llevar una mañana.

En cuanto a las subcontrataciones, y ya les he dicho que somos la firma de consultoría que más trabajamos en el ámbito de la ciberseguridad con distintas comunidades autónomas y con la Administración General del Estado, en general, con la Ley de Contratos del Estado, como adjudicatario de distintos concursos, la subcontratación se puede limitar sin ningún tipo de problema en los pliegos de un concurso a un porcentaje determinado. Incluso a la hora de pedir solvencia técnica en el concurso se puede establecer, en términos de certificaciones de persona, certificaciones de la empresa, etcétera, qué tipo de subcontratista se requiere. Ahí volvemos a lo que he comentado antes, que es la seguridad intrínseca al desarrollo de los sistemas, y en este caso hablamos de aplicaciones. Si la subcontratación o el propio desempeño profesional del adjudicatario que no subcontrata a nadie no está bien, si la aplicación no tiene una correcta seguridad en todo el ciclo de vida de desarrollo de la misma —no sé si será el caso que usted comentaba—, tendremos como resultado una aplicación que no es segura. Insisto en que desconozco el caso concreto, pero a las subcontratas, yendo ya al tema del que yo tengo conocimiento y experiencia, que es el de la ciberseguridad, como norma general ha de requerírseles por lo menos el mismo nivel de calidad en el trabajo y de garantías en certificaciones de los profesionales y de la empresa que al adjudicatario. Determinados tipos de contratos habrá que limitarlos según sea conveniente o necesario.

Creo que termino con la pregunta del retorno de los profesionales. Ha habido bastantes profesionales, en particular en el campo técnico y de las ingenierías, que han tenido oportunidades fuera, pero los

cve: DSCG-12-CM-82

profesionales de ciberseguridad tienen un punto vocacional de trabajar para las empresas y administraciones de este país. Ha habido mucha actividad y un exceso de demanda, porque es un campo en el que no se genera más empleo por falta de profesionales. En el caso de la ciberseguridad, estando totalmente de acuerdo en que si hay talento nuestro o de terceros que viene a España, estupendo, no ha habido un porcentaje significativo de talento que se haya ido fuera, aunque hay algunos casos concretos. En el caso de la ciberseguridad quizá tenemos que mirar más los temas de formación y el tema de universidades que he comentado, porque tiene todo el potencial para ser un vector de crecimiento en términos de desarrollo y de generación de empleo.

Insisto en el agradecimiento a la Comisión. Ha sido un placer pasar un rato con ustedes. Espero haber aportado un poquito de valor, que era el objetivo. Muchas gracias a todos. **(Aplausos).**

El señor **PRESIDENTE:** Señor Romero, somos nosotros los que le damos las gracias. Nos ha resultado muy útil y espero que nos sirva para avanzar en la ponencia, cuyos textos probablemente les consultaremos a todos los que han intervenido para saber si hemos sido capaces de plasmar las opiniones que se nos han expuesto.

Muchas gracias a todos.

Se levanta la sesión.

Era la una y cuarenta y cinco minutos de la tarde.

Corrección de error:

En el *Diario de Sesiones* número 73, correspondiente a la Comisión Mixta de Seguridad Nacional, sesión número 12, celebrada el jueves 14 de diciembre de 2017 en el Palacio del Congreso de los Diputados, en la página 7, cuando dice: «El señor Alonso Contorné», debe decir: «El señor Alonso Cantorné».

cve: DSCG-12-CM-82