DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2019 | XII LEGISLATURA | Núm. 126 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 25 (extraordinaria)

celebrada el miércoles 23 de enero de 2019 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

Comparecencias. Por acuerdo de la Comisión Mixta de Seguridad Nacional:

---

cve: DSCG-12-CM-126

Se abre la sesión a las diez de la mañana.

COMPARECENCIAS. POR ACUERDO DE LA COMISIÓN MIXTA DE SEGURIDAD NACIONAL:

— DEL SEÑOR DE LA CUEVA GONZÁLEZ-COTERA (ABOGADO Y DOCTOR EN FILOSOFÍA, PROFESOR ASOCIADO DE LA UNIVERSIDAD COMPLUTENSE DE MADRID), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/001552 y número de expediente del Senado 715/000616).

El señor **PRESIDENTE:** Señorías, buenos días. Vamos a dar comienzo a la sesión.

Tenemos hoy entre nosotros a don Javier de la Cueva González-Cotera, abogado y doctor en Filosofía y profesor asociado de la Universidad Complutense de Madrid para informar sobre diversas cuestiones relativas a la ciberseguridad en España. El procedimiento será el siguiente: tendrá la palabra el compareciente, intervendrán los grupos, podrá contestar el compareciente, volverán a intervenir los grupos y cerrará el compareciente. Todo eso con la brevedad y concisión propia de nuestro estilo.

Tiene la palabra el señor compareciente.

El señor **DE LA CUEVA GONZÁLEZ-COTERA** (abogado y doctor en Filosofía, profesor asociado de la Universidad Complutense de Madrid): Buenos días, señor presidente.

Señorías, qué mejor momento para cumplir treinta años de ejercicio profesional —hoy es mi trigésimo aniversario en el ejercicio profesional— que tener el honor de comparecer ante ustedes para informar de aquellas cuestiones que son producto de mi estudio. Voy a tratar un tema —me lo van ustedes a permitir— extraño en cuanto a los que se han tratado hasta la fecha en esta Comisión. Los temas que se han tratado hasta la fecha en esta Comisión, salvo uno de los ponentes —que ha sido mi compañero de profesión don David Maéztu, que habló del código fuente—, no se han referido a un estudio sobre este tipo de cuestiones que entiendo que son tremendamente significativas. Me van ustedes a permitir unir dos mundos que son absolutamente paralelos, y que es un mundo en el que vivimos desde hace doscientos años, que es el mundo de la Ilustración. Por tanto no voy a hacer una comparecencia en el sentido de lo que ustedes puedan estar habituados, de aquellas personas que nos puedan venir a decir cuáles son los problemas que podemos tener actualmente en el mundo con respecto a lo que pudieran ser los ataques externos, sino que me voy a centrar en la esencia de la democracia, debido a la existencia actualmente de un modelo de gestión y de un modelo de control que pasa por unas ciertas tecnologías, y que están eludiendo la aplicación del principio de legalidad y eludiendo aquellos principios que para nosotros y a nuestro entender son sagrados y que se consagraron en una época histórica como es la Ilustración. Por ello voy a hablar de la importancia del código fuente, y para ello les voy a iniciar con un ejemplo que es bastante —entiendo yo— canónico.

Cuando ustedes legislan sobre el Código Civil, en el Código Civil existe una disposición que nos permite la formalización, la realización o la creación de los contratos atípicos. Nosotros en el Código Civil no tenemos por qué ir a un determinado tipo de contratos que son los únicos existentes, sino que tenemos una libertad de creación. Esto no está ocurriendo en el mundo tecnológico por una serie de motivos que les explicaré a continuación. Por tanto, en primer lugar, voy a hablarles sobre en qué consiste el código fuente, su importancia y vinculación con las normas jurídicas; en segundo lugar, les voy a hablar —y me perdonarán ustedes— de la relación entre el derecho y la tecnología, y les hablaré de semiótica —les pido perdón— que es un tema bastante ajeno a la ciberseguridad, y sin embargo verán ustedes cómo está totalmente relacionado, y por último, les hablaré sobre los problemas que se plantean de la ignorancia que se está produciendo actualmente en aquel tipo de normas.

En febrero del año 2017 hubo una reunión de la vicedecana de los procuradores de Madrid, doña Rocío Sampere, con los técnicos de la Consejería de Justicia de la Comunidad de Madrid, porque a los letrados de la Administración de Justicia les aparecía en la pantalla de los ordenadores una serie de indicaciones sobre cuándo se habían producido las notificaciones realizadas a los letrados en un momento determinado en un procedimiento, y sistemáticamente aquellos letrados interponían los recursos fuera de plazo. La indicación que recibía el letrado de la Administración de Justicia en su pantalla era una indicación que había inventado el informático, que había hecho una tecnología *contra legem* —no respetando la ley— y esta tecnología, al darle una noticia al letrado de la Administración de Justicia sobre cuándo se había producido la notificación, que era realmente distinta de cuándo le había llegado la notificación al letrado

cve: DSCG-12-CM-126

contrario, provocaba que sistemáticamente se invalidara la posibilidad de cumplir los plazos procesales. Se solucionó de una manera muy sencilla, allí también estaban los técnicos de la Administración de Justicia y estos técnicos modificaron el código fuente, se tenía acceso al código fuente, y esto hizo que se pudiera modificar este tipo de problema de justicia.

Fiscalía de una provincia de Castilla-La Mancha. El fiscal jefe recibe de repente una notificación diciendo que los autos se hallan en itinerancia, y por tanto puede acceder a ellos. Cuando antes lo que hacíamos era un traspaso de todo el documento físico a la fiscalía para que pudiera empezar a calificar, ahora resulta que hay un funcionario del juzgado que aprieta un botón y se han inventado —por lo tanto ya tenemos una tecnología *praeter legem*— la existencia de una serie de maneras de proceder que no vienen tampoco en la ley y que quien las ha diseñado ha sido el informático. Por tanto, si el Conde de Romanones dijo en su momento 'haga usted la ley y déjeme el reglamento', en el siglo XXI diría 'haga usted la ley, haga el reglamento y déjeme la aplicación informática'. Porque si obligo a los ciudadanos a realizar su declaración de la renta a través de una aplicación informática, y soy el informático y quito la casilla de la deducción por hijos, acabo de cambiar la ley y el reglamento. Por lo tanto nos encontramos con que de hecho se están produciendo unos sistemas de legislación, unos sistemas de producción de normas jurídicas con incidencia absoluta en todos los derechos fundamentales y ordinarios de los ciudadanos que está en manos de personas que no están habilitados por la ley para legislar. Esto lo estamos viviendo hoy en día.

Esta producción normativa se está dando en dos campos de actuación de las administraciones y de los poderes del Estado, que son: en primer lugar, técnicas de gestión, y en segundo lugar, técnicas de control. Cuando voy por la carretera y tengo dos radares en tramo yo no puedo como ciudadano tener acceso al código fuente para verificar si los dos radares tienen el horario sincronizado, porque si el segundo de los radares tiene cinco minutos adelantado su temporizador resulta que voy a ir a 360 kilómetros por hora a lo mejor en un 600, que ya es un vehículo histórico. Por lo tanto nos encontramos con que este tipo de técnicas se están realizando en el supuesto de los impuestos en Administración, pero en el supuesto de los coches, de los radares de control mediante un determinado tipo de código. Ahí nos estamos encontrando con un código al cual nosotros no tenemos acceso, que está produciendo efectos jurídicos que en muchas ocasiones se está normativizando —tiene las capacidades normativas de los lenguajes naturales—, y sin embargo mediante la existencia de estos lenguajes formales estamos realizando una producción normativa. Hasta ahora siempre hemos legislado en lenguajes naturales, y estos lenguajes naturales tienen una relación con la tecnología de la escritura esencial.

En un momento determinado —y aquí ya entramos en periodo griego, y no me voy a extender en ese aspecto— lo que se empieza a realizar es una positivización de las normas. La norma se escribe, y se escribe —según dicen todos los autores clásicos, Rodríguez Adrados o Guthrie, por ejemplo— para evitar su arbitrariedad, para que la norma ya esté fija. Cuidado, cuestiones aparte ya serán los problemas hermenéuticos derivados de esa fijación de la norma. Pero ya hemos quitado dos problemas, la existencia de la norma ya queda fijada mediante una tecnología que, según Mosterín, es esa tecnología de dibujar los sonidos. Nosotros dibujamos los sonidos y la tecnología de la escritura es quizá la más importante y la más poderosa que jamás se ha podido escribir. En esta tecnología de la escritura luego, en la época de la Ilustración, se produce un acto político que es la fundación de los boletines oficiales del Estado, donde se tienen que publicar las normas. Las normas por tanto no solamente se tienen que escribir, sino que además se tienen que publicar; y no solo se han de publicar, sino que han de hacerlo en un lugar accesible y conocible absolutamente a todos los ciudadanos, porque únicamente desde ese punto se producen dos efectos. En primer lugar, evitamos la arbitrariedad del poder, y en segundo lugar, podemos exigir que alguien conozca el contenido de las normas jurídicas. Por lo tanto, tiene dos efectos: *ius civilistas* e *ius publicistas*. *Ius publicistas* en cuanto a la generación de todos los derechos de los ciudadanos e *ius civilistas* —aquí siguiendo a Liborio Hierro— en cuanto a dos efectos que son fundamentales en el Código Civil. El primero de ellos es que lo que se realiza es la costumbre, que solo puede derogarse por una costumbre posterior. Y en segundo lugar, una ley no puede quedar derogada por su desuso. Por lo tanto, entre la tensión que existió durante prácticamente mil ochocientos, mil novecientos años entre la ley y la costumbre queda evidenciado que es la ley positiva, que viene refrendada en una publicación, que es conocida por todo el mundo y que los ciudadanos tienen capacidad de conocerlo, la que tiene posibilidad de que cuando se me aplica un norma yo esté respetando el principio de legalidad. El principio de legalidad por tanto única y exclusivamente es posible en el momento en el cual yo tengo la realidad de poder de conocer la norma. Epistemológicamente puedo conocer y tengo acceso a esta norma jurídica.

cve: DSCG-12-CM-126

¿Está ocurriendo esto hoy en día? No, señorías. Y este es el grave problema que atañe a la seguridad. No es una seguridad nacional solamente en cuanto a que no tengo acceso al código fuente del *software* de los carros de combate o de los aviones de combate; no tengo acceso al código fuente de todo aquel *software* que esté gestionando o administrando todas aquellas infraestructuras estratégicas del Estado; no tengo acceso ni siquiera al código fuente como ciudadano para poder discutir una resolución que se hubiera podido fundamentar en la aplicación de un determinado tipo de *software*. Y aquí permítanme que entre en semiótica. El ejemplo clásico que en semiótica se utiliza es el del semáforo. Y en semiótica existen tres capas. La primera es la sintáctica, que son los elementos, los signos con los cuales nosotros podemos construir un determinado tipo de lenguaje. En un semáforo tenemos simplemente tres signos: el color rojo, el amarillo y el verde. Y esos tres signos tienen además unas reglas de combinación. Primero va el rojo, luego va el verde y luego va el amarillo. Hay veces que el amarillo puede estar intermitente, pero no tenemos de repente el rojo y el verde haciendo funciones discotequeras; lo que tenemos es una sintaxis con unos símbolos que están establecidos, es un establecimiento más universal. Sintácticamente el universo conoce qué significa el rojo, qué significa el amarillo y qué significa el verde. Perdónenme ustedes, el rojo y el verde está muy claro su significado; con el amarillo existe una costumbre según los lugares de o acelerar, que se va a poner rojo, o parar, que se va a poner rojo. Según la cultura de donde estemos aplicando esta simbología se va a producir un efecto u otro. El norte de España no es igual que el sur de España, y sus señorías lo conocen. La segunda capa, además de la sintáctica, es la semántica y aquí es donde entra el derecho. El derecho lo que nos está diciendo es que al color rojo le asignamos una prohibición de pasar y al color verde le asignamos un permiso de pasar. Y la tercera de las capas, ya no es la capa semántica que es lo que significan esos signos, sino la capa pragmática que consiste en qué tipo de mundos podemos nosotros construir con ese tipo de colores, con esa sintaxis. Y con una sintaxis tan básico como pudiera ser el rojo, el amarillo y el verde lo que hemos construido son rotondas, calles, pasos de cebras, *stops*, hemos decidido dónde se instalan los semáforos y dónde no. Todo el mundo habla del arco de triunfo y obviamente aquí en España tenemos que hablar de nación rotonda. Les aconsejo la visualización de una web que se llama Nación Rotonda, donde se verifica todo el impacto pragmático que ha tenido dentro de un diseño urbanístico simplemente la existencia de tres colores. Por lo tanto una de las funciones pragmáticas de la sintaxis es la creación de mundos, qué mundos son en los que yo puedo vivir.

La tecnología, señorías, no es un imponderable al cual yo me tengo que someter. La tecnología permite precisamente la actividad humana. Decía Ortega que precisamente la tecnología tiene un método, y este método es en el que nosotros podemos decidir o no si intervenimos según qué tipo de parte de la semiótica nos permite intervenir. Si yo puedo intervenir a nivel sintáctico el mundo que yo puedo construir es riquísimo; si yo puedo intervenir a nivel semántico el mundo que yo puedo construir ya tiene unas limitaciones, y si yo solamente puedo intervenir en un mundo de una manera pragmática no tengo prácticamente ningún tipo de opciones, porque ya la arquitectura del sistema es la que me está dotando de las posibilidades de lo que yo puedo hacer. Por tanto, cuando yo puedo intervenir en una tecnología es cuando yo dispongo del código fuente. Si me dan un Código Civil y lo que me dicen es: no, usted no puede utilizar más contratos que los que ya vinieron en el código civil francés y usted no puede modificar ningún artículo, yo no podría construir un mundo jurídico y no podría construir los derechos y obligaciones del comprador y del vendedor, porque ya serían los que me vendrían dados. Sin embargo en la situación en la que yo me encuentro con la tecnología ese es el supuesto que tenemos, y no lo discutimos, lo damos por hecho, es algo que nos viene dado, y por tanto nosotros no podemos intervenir en esa elaboración.

Permítanme ustedes que cite a Wittgenstein, que decía: Los límites de mi lenguaje son los límites de mi mundo. *Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt.* Esto es lo que está ocurriendo actualmente. Cuando Apple nos enseña una publicidad y nos dice que usted puede hacer lo que quiera, y que lo importante es lo que está por el ordenador, lo siento mucho, nos están desenfocando la mirada. Porque la mirada la tenemos que poner en la configuración del ordenador y lo que a mí me permiten hacer con el ordenador. Y aquí me voy a la siguiente cuestión. Cuando ustedes acceden a su cargo se les dota de unos medios tecnológicos. ¿Qué saben ustedes de dónde envían información esos medios tecnológicos? Ustedes son la representación de la soberanía popular, y cuando nosotros nos encontramos en la página web del Congreso de los Diputados el símbolo de Facebook, el símbolo de Twitter y demás símbolos de redes sociales yo lo que siempre me planteo es: el Congreso de España, igual que el jefe del Estado —esta fue una pregunta que hice ante el portal de transparencia—, simplemente haciendo clic ha aceptado los términos y condiciones de Twitter y de Facebook, y por tanto en el caso de Twitter se ha

cve: DSCG-12-CM-126

sometido a la jurisdicción de los tribunales de California y a sus normas. Y yo pregunté qué abogado del Estado ha sido el que ha autorizado que la Casa Real, que nuestro jefe de Estado se haya sometido a una jurisdicción extranjera. La respuesta que obtuve fue que bueno, que la vida es bella. Esto es algo que merece nuestra atención como juristas, es algo que nos obliga a comenzar a exigirle a todo aquel *software* que se utilice para las administraciones públicas o para los poderes del Estado y que tengan dos funciones, la función de gestión y la función de administración, que contengan las mismas características que la generación de las normas jurídicas. En primer lugar, un cuerpo de personas, de representantes que sean quienes las lleven a cabo; en segundo lugar, se tiene que realizar en unos repositorios abiertos al público donde los ciudadanos, en el ejercicio de su deber y su derecho de participación, puedan hacer las alegaciones correspondientes al código, y en tercer lugar, este código no puede ser un código propietario, no puede ser propiedad de nadie. El artículo 13 del Texto Refundido de la Ley de Propiedad Intelectual lo que establece es que las normas jurídicas y las resoluciones judiciales, entre otros textos generados por el Estado, son de dominio público, y por tanto la norma jurídica es de dominio público, y en consecuencia el *software*, todo aquel *software* que esté realizándose por un órgano estatal tiene que ser también de dominio público. Ni siquiera tiene que ser *software* libre, ni siquiera —dicen— *software* abierto, código abierto. No; tiene que tener la misma naturaleza jurídica que tienen las leyes, y por ello toda la teoría de las fuentes del derecho ha de aplicarse al código jurídico.

Termino, señorías, sintetizando simplemente estas cuestiones porque las quiero dejar bien claras. En primer lugar, debe existir una regulación jurídica que establezca qué órganos tienen competencia para la escritura del código fuente y de los algoritmos —a los que los ciudadanos también tenemos que ser capaces de tener acceso, porque de ellos depende la aplicación de las normas jurídicas—, así como el procedimiento sobre su labor. La causa de esta cuestión la encontramos en el filósofo italiano. Ferrajoli nos dice que los procedimientos de formación de los actos legislativos también forman la democracia. Yo quiero saber la norma jurídica que se me aplica, quiero tener derecho a mirarla. Yo sé leer código fuente, señorías, soy abogado; sé leer código fuente en Código Civil y sé leer código fuente según determinados tipos de programación. Pudiera no saberlo, bien, pero es que en 1800 el 30 % de los aristócratas españoles eran analfabetos, y no por ello tendríamos que decir que las leyes no tuvieran que estar escritas. Ya tendré yo a alguien que pueda leer por mí, y de ahí la figura del procurador, que era una persona que sí que tenía que ser letrada, tenía que tener la capacidad de leer esa tecnología para poder representar a la persona que no podía ser letrada. En segundo lugar, este permiso que se tiene que hacer a la ciudadanía de alegaciones se tiene que producir desde el principio del inicio de la norma, porque los repositorios tienen que ser públicos, como el producto de esta Comisión se está retransmitiendo ahora mismo por *streaming*. Esto se tiene que hacer con la producción normativa que sea de lenguaje de tipo formal. En tercer lugar, la razón de todo esto es el artículo 23.1 de la Constitución española, que es el derecho de participación que todos tenemos en aquellas normas que nos afectan. En cuarto lugar, el código fuente y los algoritmos se deben publicar en repositorios oficiales para que podamos leerlos. Por último, conforme ya en el año 2012 la doctora Elena Nadal y yo propusimos en un artículo académico publicado, el código fuente y los algoritmos, al igual que la ley y la jurisprudencia, tienen que ser de todos nosotros. Esto además —vuelvo a la Ilustración— cuando Kant en *Sobre la paz perpetua* lo que nos dice es que la paz de una sociedad depende de dos tipos de interacciones, la primera de ellas es la interna. No podemos tener una arbitrariedad del poder, el poder tiene que ser transparente para que podamos evitar esta arbitrariedad. En segundo lugar, tiene también una aplicación externa. Dice Kant que cuando un Estado es transparente también evita las guerras con los Estados de fuera. Ralf Dahrendorf también lo dice, condiciones de la democracia, cuando hay democracias hay menos guerras entre las democracias y los demás Estados. La soberanía tecnológica de un Estado depende precisamente de su capacidad de ser transparente con respecto al código fuente de los programas que realizan esas dos labores de gestión y control. Ese código fuente por tanto es algo que tendremos que empezar a exigir.

Sé que esto no lo vamos a lograr, quizás dentro de cien años empecemos a plantearlo. Pero, en palabras de Norberto Bobbio, quizá lo que estemos haciendo sea, al igual que con los derechos fundamentales al principio, tener ideas, y lo que buscamos son organizaciones que las adopten, que las acojan y que las hagan suyas.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias.

Vamos a dar la palabra al representante del Grupo Ciudadanos, señor Salvador.

cve: DSCG-12-CM-126

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

En primer lugar, quiero felicitar al señor De la Cueva por su aportación, porque es cierto que a esta altura de la realización de los trabajos de esta Comisión es complicado decir algo nuevo, pero lo que usted ha dicho es totalmente distinto a lo que ha dicho cualquier compareciente anterior. Por tanto ha aportado algo que debe ser tenido en cuenta evidentemente. Me quedo más con la parte filosófica de su intervención que con la aportación sobre el concepto de la ciberseguridad porque, por una parte, su discurso me ha recordado la etapa 2005, 2006 cuando estuvimos promoviendo el Plan Avanza para el desarrollo de la sociedad de la información y el debate que había en ese momento sobre el *software* libre y el *software* propietario. Ese debate era de calado y los defensores no eran unos simples frikis que lo que querían era tener la capacidad de poder jugar y toquetear los sistemas, y a partir de ahí poder tener esa participación, sino que lo que se pretendía era evitar y se criticaba que si comprabas un *software* propietario no sabías qué gobierno te podía estar espiando o qué podía suceder con esa información que tú estabas gestionando como país. Pero quiero recordarle también que uno de los problemas que tuvimos en ese momento, y que afecta también a eso que usted está diciendo hoy, era que incluso en la Administración General del Estado no había un estándar que hiciera que los sistemas que se utilizaban en las bases de datos fuesen comunes. Eso dificultaba la gestión de la Administración General del Estado con el propio Tribunal de Cuentas a la hora de poder suministrarle información económica. Lo primero que hubo que hacer fue crear un estándar para que toda la Administración tuviera que trabajar con el mismo. Si nos vamos más adelante lo vemos con la sanidad, la receta electrónica y el historial clínico. Por tanto hay soluciones *ad hoc* desarrolladas por quien tiene la competencia, que es cada comunidad autónoma, cuando lo lógico es que haya un sistema que afecte a todos y que tenga todas las garantías, en la línea de lo que usted está planteando.

¿Por qué le digo eso? Porque la tecnología siempre ha ido por delante, no digo que sea bueno o malo, pero la tecnología siempre ha ido por delante de la norma. No se ha hecho una norma para una tecnología que iba a llegar. Nos hemos encontrado con una tecnología que estaba implantada o se estaba desarrollando, y a partir de ahí nos hemos puesto a trabajar y pensar cómo podemos hacer una norma que regule esa tecnología. Por poner un ejemplo de lo que estoy hablando hay que decir que las redes sociales surgen como un ámbito más abierto que conecta también a las personas y a las instituciones con el mundo exterior, mucho más allá de una página web corporativa o de un programa o una aplicación que desarrolle tal servicio. Por ejemplo, la Casa Blanca y el presidente Obama, que no fue el primer presidente en empezar a utilizar redes sociales, pero sí la persona que la gente entendió que asumía como presidente de un país la defensa de la utilización de las redes sociales para comunicarse con los ciudadanos, cuando entrabas a la web de la Casa Blanca entrabas a esa web con su *software* y cuando te ibas a conectar al Youtube del presidente, al Twitter del presidente o a cualquier *flickr* del presidente, te salía un mensaje que decía: usted está a punto de abandonar los servidores de la Casa Blanca y va a pasar a operar con el servidor tal. ¿Para qué? Para que la gente no pudiera exigir responsabilidades a la Casa Blanca de lo que pudiera suceder en ese entorno de Twitter, de Facebook o cualquier otro operador. Por eso le digo que la tecnología siempre va por delante, lo estamos viendo con las tecnologías disruptivas en lo que van a afectar al empleo y a muchísimos ámbitos de la sociedad, y en los que todavía no estamos trabajando en preparar ese mundo que va a llegar para proteger al trabajador y no al puesto de trabajo. Esto lo digo porque son debates que están por llegar, pero que ya podríamos estar anticipando.

Todo lo que usted ha comentado en su intervención me hubiese parecido muy oportuno haberlo escuchado al principio de este debate, no ya de la Comisión de Ciberseguridad, sino de todo el debate que se está manteniendo, porque desgraciadamente en este momento la ciberseguridad es un campo de batalla, es decir, se necesita ciberseguridad para proteger sistemas, para defenderse de ataques, para proteger a ciudadanos. Usted ha hablado antes de la Administración, pero la Administración tiene un poder más importante que el ciudadano que se conecta a un móvil o a una aplicación determinada o utiliza una red social. Esa persona es susceptible de que le roben su información, de que le suplanten su identidad, de que cometan delitos contra ella. Por tanto ahí no cabe código fuente ni ser propietario, porque esas personas están utilizando sistemas usados mundialmente. Por ello quiero pedirle —aunque sé que es difícil siempre que se hacen intervenciones como la suya, por eso digo que me quedo con la parte positiva, por mi parte fantástica su intervención— que haga lo más complicado, que es bajar de la teoría a la praxis. Conociendo cómo funciona la Administración pública española, que creo que es a la que usted se refiere más con el control del código fuente —repito, es muy complicado controlar el código fuente en el mundo abierto, con las multinacionales y cómo está gestionado—, qué aportaciones prácticas entiende usted que se podrían desarrollar hoy dentro de nuestras administraciones para que esta Comisión pudiera incluirlo

cve: DSCG-12-CM-126

en sus conclusiones, pudiéramos tratar de llevarlo a un Pleno o a Comisión para aprobar una medida en la que instemos al Gobierno a hacer qué, porque si no lo que estaríamos reconociendo es que la pérdida de control de ese código fuente, con todo lo que usted ha puesto a su alrededor a nivel filosófico y real, es una frustración o una queja, pero de difícil solución. Sí le pido que intente concretar de la teoría a la praxis, y así estoy seguro de que esta Comisión va a salir ganando con sus aportaciones.

El señor **PRESIDENTE:** Gracias, señor Salvador.
Tiene la palabra la senadora Angustia Gómez, de Unidos Podemos-En comú Podem-En Marea.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Buenos días, señor De la Cueva. Gracias por su disponibilidad para asistir a esta Comisión, y sobre todo muchas gracias por su trabajo, que ha sido fantástico en la exposición, y seguramente tenga mucho que ver con que usted haya seguido la ponencia y haya intentado de forma totalmente intencionada preparar su trabajo para aportarnos algo totalmente nuevo. Creo que es algo que hay que valorar y en nuestro grupo parlamentario se lo agradecemos. Enhorabuena también por el aniversario de su ejercicio profesional y nos alegra poder celebrarlo con usted.

Hace aproximadamente un año medio oí por primera vez hablar sobre ello en una web que se utiliza habitualmente para preguntas y respuestas de programadores, una web que se llama Stack Overflow y que posiblemente es la más conocida. Se hizo una defensa —yo no sé si interesada o no, no entro en eso— muy interesante sobre cuál era el lenguaje de programación de futuro, cuál era el que ofrecía más garantías y, sobre todo, que es precisamente lo que me pareció interesante en este artículo, cuál era el que ofrecía más posibilidades de desarrollo para el *big data*, que en este momento era como el *mainstream* de la gestión de datos. Como ustedes conocen muy bien Python, y era precisamente de lo que hablaba este artículo, lo que hacía era defender Python como el mejor lenguaje de programación para el *big data*. Muchas veces —lo sabe porque ha seguido las sesiones de esta ponencia en la Comisión de Seguridad Nacional— se ha hablado de *big data*, pero nunca desde el punto de vista de la programación y a la ponencia le resultaría muy interesante saber si de verdad hemos determinado, o los especialistas y las especialistas han determinado, por la experiencia y por el uso de Python que usted hace habitualmente, si no me equivoco. Creo que sus *scripts* los escribe habitualmente en Python, existe una tendencia a considerar que la seguridad, el *big data*, que es imprescindible para la recopilación, el tratamiento y la gestión y difusión de la información, de eso que estamos hablando, es de verdad el sistema más seguro, y en caso de serlo, cuáles son los argumentos que se utilizan para decir no solo que ahora mismo sería el lenguaje de programación más seguro, sino que además es el que tiene más recursos de futuro y, por tanto, aportaría una mayor continuidad al desarrollo de sistemas.

A partir de ahí me cambió totalmente de tercio porque creo que si hay algo interesante en su experiencia laboral es precisamente ese marco mixto de ejercicio profesional y docencia que tiene. Hemos hablado muchas veces de formación y creo que nos interesa a todos los grupos parlamentarios que, de un modo u otro, hemos manifestado nuestro interés por la formación. Es cierto que no estamos de acuerdo en cuál sería la mejor forma de hacerlo, pero sí en que hay que mejorar nuestra formación y, sobre todo, la formación superior, y me voy a detener en este punto. Muchas veces se habla de especialización. En los últimos tiempos, de hecho, muchos de sus artículos académicos o divulgativos han versado precisamente en torno a la especialización porque es necesaria. ¿Qué podría aportar y, sobre todo, cómo tendríamos que adaptar nuestro sistema educativo para que esta formación tendiese a la especialización?

Hay otro tipo de formación de la que se habla muy poco que es el objetivo de formación continua que debería de tener absolutamente todo el personal de la Administración pública respecto de la tecnología, del uso, de la gestión de información y de la seguridad. ¿Qué podríamos mejorar en este campo?

Le pido su opinión sobre una cuestión en la que tampoco nos ponemos de acuerdo, pero que continuamente está saliendo y tiene que ver con la formación, la especialización y la canalización del talento. Creo que no son lo mismo los *hackers* que los *crackers* y hay quien cree que sí. Los *crackers* no son delincuentes sino talentos con una gestión individual de ese talento que posiblemente se podría canalizar para que sus aportaciones fuesen positivas para el conjunto. Me gustaría saber su opinión y cómo cree que se puede canalizar este talento en personas que *per se* ya se están especializando en determinados campos pero luego no utilizamos su talento.

Termino hablando del código fuente, que es sobre lo que usted ha venido a formarnos y a ayudarnos para que la ponencia sea lo más completa posible. El problema de Lexnet fue precisamente que la arquitectura, el sistema y el código fuente se filtraron. No solo no era seguro sino que además tenía

cve: DSCG-12-CM-126

muchísimos problemas a lo largo de la utilización de todo el sistema. ¿Necesita la Administración de Justicia algo especial cuando estamos hablando de TIC, algo que no tuviese, necesita Lexnet, necesita la Administración de Justicia alguna especificidad que no se está teniendo en cuenta en la resolución de problemas y para tener un sistema no solo seguro ni de futuro? Lexnet ejemplificó muy bien un problema que no conseguimos resolver que es la falta de comunicación y de seguridad hacia la ciudadanía. O bien nos equivocamos en cómo enfocamos las relaciones o bien nos equivocamos en lo que comunicamos, pero parece que no se consigue generar toda la seguridad que debiese en la opinión ciudadana. Parece que hay un problema de enlace entre los poderes públicos y la sociedad y también tal vez tenga alguna idea al respecto de cómo podemos comunicar correctamente y cómo esa relación en torno al mundo tecnológico entre los poderes públicos e incluso en las empresas puede mejorarse con el conjunto de la sociedad.

Muchísimas gracias.

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

Señor Luena.

El señor **LUENA LÓPEZ:** Gracias, señor presidente. Buenos días, señorías.

Profesor De la Cueva, muchas gracias y felicidades por su aniversario. Le voy a pedir en primer lugar, ya que nos ha servido de inspiración esta mañana, que nos sirva también de inspiración a la hora de poder tener, si cabe, con más desarrollo y amplitud, que seguro que los tiene, esos textos que hoy ha utilizado en esta comparecencia para que puedan servirnos de base de una posible parte de introducción de la ponencia porque creo que hay principios inspirativos, reflexivos y filosóficos como los que usted ha expresado en esta sesión de esta Comisión esta mañana nos vendrían muy bien.

Usted sabe lo que ha hecho porque lo ha hecho deliberadamente y yo le felicito. Suele decirse que teníamos las respuestas y ahora nos cambia las preguntas. Usted ha venido aquí a cambiar las preguntas y todavía no teníamos las respuestas, le informo: en esta Comisión, todavía no. Tenemos bastante trabajo desarrollado y bastante acervo, pero no tenemos las respuestas y usted ha venido y nos ha cambiado las preguntas.

Le voy a hacer algunas preguntas tanto de derechos, que usted ha empleado, como de ciberseguridad porque esta es una ponencia de ciberseguridad. Algunas usted no las ha introducido en su intervención y estamos en el Grupo Parlamentario Socialista muy interesados en conocer su opinión. En primer lugar, a la reflexión que usted hace yo le hago otra del profesor Harari. Usted ha hablado de la creación de dos mundos y Yuval Noah Harari, que ha escrito *sapiens* —todo el mundo lo sabe—, llega a decir en su último libro —y ya lo adelantaba en *Homo Deus*—, en *21 lecciones para el siglo XXI*, que al final el dataísmo —como lo llama él—, la fragilidad de la utilización de los datos y la tecnología va a llevar a que haya dos niveles dentro de la subespecie *sapiens* y va a haber una que esté por encima en el uso de las capacidades tecnológicas y otra que esté por debajo, y ahí sí que de verdad va a haber una ruptura de la especie. No le pregunto si usted cree que va a haber una ruptura de la especie, pero si cree que, dada la fragilidad de la utilización de los datos, finalmente los *sapiens* vamos a ser capaces de manejarlos o vamos a ser manejados por los datos. Porque también, en función de eso, las políticas públicas institucionales de ciberseguridad, al menos en ese marco, como usted ha dicho, de la ilustración o de esta era de la posilustración, tendrán que legar a las generaciones siguientes algo en lo que fijarse cuando les toque tomar responsabilidades. Aspiramos a que una de las cosas en las que se fijen sea la ponencia de esta Comisión.

A partir de ahí, si me permite, le voy a hacer una ensalada de preguntas concretas, algunas de carácter muy político como, por ejemplo, respecto a las grandes corporaciones, porque al principio de todo esto —ahora hablaba de esto con mi compañero Juan Carlos Raffo— están las grandes corporaciones, está el capital. ¿Usted es favorable, por ejemplo, a que se pongan los impuestos que se van a poner ahora a las empresas digitales? ¿Qué opina usted de las multas? ¿Le parecen duras, le parecen blandas, como, por ejemplo, las que ha tenido Facebook, precisamente por el manejo de los datos? ¿Puede darnos alguna opinión —ahora o por escrito— también sobre la Directiva de ciberseguridad de la Unión Europea? Creo que no lo ha mencionado, pero, si lo ha hecho, le pido disculpas porque no lo escuchado.

En relación con España, a algunos que han venido aquí les hemos pedido que pusieran nota al esquema de seguridad de España. Seguro que ha leído mucho sobre esto. A todos nos gustan mucho las listas. Siempre nos han dicho —cómo no, también en ciberseguridad— que Estados Unidos e Israel estaban los primeros. ¿Dónde cree usted que está España, teniendo en cuenta su valoración, en primer lugar, sobre la coordinación que existe con el sector privado —lo que usted conozca o haya leído— y la estructura que tenemos de ciberseguridad en España? ¿Cuál cree usted que es el nivel comparativamente, en política comparada? Y si ya pudieran decirnos hoy o para el futuro en esta ponencia las fortalezas y

cve: DSCG-12-CM-126

vulnerabilidades, se lo agradeceríamos. Al señor Maeztu, que también hizo una intervención similar a la suya y nos habló de las deficiencias, del déficit que tenían las administraciones, yo le pregunté por una que nos preocupa mucho a los socialistas, que es la vulnerabilidad en el ámbito local. Me gustaría que usted nos dijera cómo lo ve.

¿Qué le parece el presupuesto? No me refiero al de este año o al del anterior, sino a la evolución presupuestaria, la serie presupuestaria del Estado español, que es menor, según nos dijo aquí un alto mando del ejército, respecto a no sé qué gran empresa o gran banco —no recuerdo cuál dijo—, porque se gasta más en ciberseguridad de lo que se gasta el Estado español. No sé cómo valora usted esto.

En cuanto al tema de los cibervoluntarios —ahora la compañera de Unidos Podemos ha terminado diciendo algo parecido—, ¿usted cree que es buena su regulación, como ya le han preguntado? ¿Cómo ve la frontera con la ciberdelincuencia? En esta Comisión estamos muy preocupados por la formación; hay responsables del Gobierno que nos han ilustrado sobre la necesidad de formar un cuerpo de personas que estén en la ciberseguridad más allá de los voluntarios. ¿Usted tiene ideas sobre cómo podría ser, por decirlo de alguna forma, un plan de estudios de formación?

Voy terminando. En el ámbito de la legislación, además de las cosas que usted nos ha dicho sobre el código fuente, ¿cree que sería necesaria una carta específica de derechos y deberes digitales? También se lo hemos preguntado a algunos de sus compañeros.

Como le decía, termino con una pregunta de carácter político. ¿Qué opina usted sobre las injerencias que se ha dicho que ha habido o que pudo haber en la política nacional? Las ha habido en Estados Unidos, como se está demostrando, y hay un fiscal que está investigando; y aquí, en política nacional, concretamente en la crisis catalana, utilizando huecos de la tecnología, la Federación Rusa parece que intentó intervenir. Yo no sé si usted tiene información o conocimiento acerca de esto, pero me gustaría que nos dijera cómo se pueden prevenir estos ataques.

Termino con algo que está siempre en el orden del día de todos los grupos parlamentarios y de los portavoces que toman la palabra de esta Comisión. ¿Hasta dónde llega no la conciencia de estar en una nueva etapa de la humanidad, como decíamos al principio, sino la conciencia de riesgo práctico, de la fragilidad de los datos, de los pasos que damos en la doble vida real digital en la que vivimos, no solo en las instituciones sino también socialmente? Esta es la última pregunta que quería hacerle.

Concluyo pidiendo —seguro que lo harán— a la Mesa y a la Presidencia de la Comisión que nos manden los textos porque nos vendrán muy bien para trabajar en la ponencia.

Muchas gracias.

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

La última interviniente, otra *sapiens*, es la señora Cabezas.

La señora **CABEZAS REGAÑO:** Gracias, presidente.

Buenos días, señor De la Cueva, y muchísimas gracias por su intervención, que es verdad que ha sido algo diferente a lo que habitualmente hemos escuchado en esta Comisión. Casi todos los ponentes en las distintas comparecencias coinciden al final en una parte que yo creo que es la más importante, y es que estamos expuestos a muchos riesgos y que además no tenemos todavía la ciberseguridad al cien por cien. Es importante tener esto en cuenta para poder seguir trabajando en esa seguridad que queremos, no solamente, como usted ha mencionado, para la política sino para cualquier ciudadano. Como ya he dicho en otra sesión anterior de esta Comisión, primero llegó la tecnología y después la educación en ella y, por lo tanto, llevamos un gran retraso porque la tecnología está avanzando a un ritmo que es demasiado rápido para ponernos al día. Corremos muchos peligros cuando apretamos un botón: la mayoría de las veces ese gesto es de gran utilidad pero conlleva muchos riesgos, riesgos que no conoce la sociedad en general, y ya no solamente hablo de las administraciones sino también de cualquier persona normal y corriente que utiliza las redes sociales o su correo electrónico con total naturalidad, pensando que nadie puede jamás entrar en esa privacidad, pero hoy —usted lo ha dicho muy bien— volvemos a ver que eso no es así. Además, en cualquier punto del mundo puede haber un *hacker* —ya lo ha dicho en su intervención— que usurpe nuestra identidad, como poco, porque pueden producirse muchísimos delitos ya que la ciberdelincuencia está siendo un gran problema y por eso en el Grupo Parlamentar Popular creemos que la ciberseguridad debe ser una política de Estado para que todos podamos trabajar juntos ante los desafíos que la sociedad nos reclama porque están produciéndose delitos verdaderamente graves.

Me ha parecido muy interesante su intervención porque nos ha abierto un mundo nuevo dentro de todo lo que está ocurriendo y por eso me gustaría hacerle varias preguntas y que usted nos hiciera una

cve: DSCG-12-CM-126

valoración desde que empezó todo el mundo de Internet, de las redes sociales, al día de hoy: en qué hemos avanzado, cuáles han sido las estrategias, el desarrollo de todo lo que ha conllevado entrar en las nuevas tecnologías y dónde estamos fallando, cuáles son los puntos todavía débiles en los que debemos trabajar no solamente a nivel público sino también a nivel privado porque las empresas se están poniendo al día y están haciendo una gran inversión para protegerse. Le agradecería que me lo explicara. También me gustaría que nos hiciera una valoración sobré qué canales de cooperación con las administraciones tanto públicas como privadas considera que pueden ser mejorados y en qué sentido.

Igualmente, hay una parte fundamental, de la que hemos hablado en muchas ocasiones, que es la educación en las tecnologías. Es verdad que tenemos muchísimo talento en España pero debería ser utilizado de manera distinta a cómo se está utilizando. Quisiera que usted, que viene de la docencia, de la universidad, nos explicara a todos si ve conveniente que hubiera un grado de ciberseguridad, dado el uso que ahora mismo la juventud da a las redes sociales, que les encantan, y algunos son verdaderos expertos sin haber estudiado, como yo he comprobado. ¿Usted cree que sería importante que el Estado hiciera esa inversión para canalizar todo ese talento en beneficio de todos los ciudadanos no solamente en política? Es verdad que escuchándole atentamente me han sorprendido muchas de sus apreciaciones en su intervención porque cuando usted ha puesto el ejemplo del semáforo. Lo he escuchado atentamente porque aquí se ha hablado de otros temas un poco más caseros y no tan caseros. Yo realicé una comparecencia sobre el mundo del voluntariado en ciberseguridad porque en Colombia uno de los comparecientes hizo esa prueba allí y más de 100 000 personas son voluntarios en ciberseguridad. Allí ha dado un resultado extraordinario porque no solamente tenemos derecho a utilizar el ciberespacio y todas las redes sociales sino que también tenemos obligaciones y a la mayoría de los ciudadanos lo que nos pasa es que creemos que tenemos todos los derecho del mundo pero que no tenemos ninguna obligación con respecto a su buena utilización.

Asimismo, hay algunos compañeros que se han extendido en algunas preguntas que yo también le iba a plantear, pero a mí me gustaría detenerme en un aspecto en el que pueda trasladarme tanto a mí como a los padres algún consejo en cuanto al mundo de la infancia, aspecto que siempre he planteado en las comparecencias, porque nuestros niños están expuestos a unos peligros bastante brutales. Me gustaría que nos diera algunos consejos sobre cómo seguir informando a esos padres, a esos niños, a esos adolescentes de los peligros que conlleva el mal uso de las nuevas tecnologías, y también al profesorado. Es verdad que nuestras Fuerzas y Cuerpos de Seguridad del Estado están haciendo un gran trabajo en informar a través de charlas, pero no muchos padres tienen en cuenta ese tipo de charlas y creo que hay que hacer un buen trabajo en seguir informando y sobre todo en hacer hincapié en la gran exposición que tienen esos niños y niñas en la mala utilización de las redes. Desde su experiencia, desde su conocimiento, nos gustaría que nos informase al respecto, o a mí por lo menos me gustaría para poder trasladarlo a mi provincia. Yo soy de Córdoba y además pertenezco al mundo rural, y con eso quiero decir que las redes sociales pueden estar muy bien, pero la información para evitar una mala utilización muchas veces no llega. Me gustaría poder llegar mañana a mi pueblo y volver a reiterar a tantos jóvenes, a tantos niños, a tantos padres del gran peligro que tenemos.

Con respecto a ese código fuente, usted ha dicho que si a la Administración aún le cuesta trabajo porque quizá no se estén haciendo las cosas bien y hay que seguir trabajando en ese modelo de ciberseguridad, imagínese a una familia del mundo rural donde personas con setenta, ochenta o noventa años que utilizan las redes sociales pero que no saben realmente el peligro que conlleva el que puedan usurparles su identidad, entrar en su correo, en sus redes sociales y hacer cosas que verdaderamente no harían. Me gustaría detenerme en este aspecto y que me diera esos consejos que yo podría trasladar a todos los vecinos de mi municipio.

Ya se le han hecho muchas observaciones y preguntas, pero me gustaría plantearle otra. ¿Qué perfiles de talento podría describirnos con el fin de modificar esos planes de estudios, que usted anteriormente ha dicho que podrían servir, tanto a nivel universitario como de formación profesional para dar respuesta a un mercado que, según nos han informado muchos comparecientes al igual que usted, es deficitario en la actualidad de muchos de estos perfiles, tanto en ciencia como en matemáticas, como se ha dicho en alguna comparecencia? Me gustaría que usted nos diera también su valoración y sobre todo si sería bueno empezar a trabajar ya en ese nuevo grado y que pudiera implantarse en nuestras universidades para que nuestros jóvenes puedan tener esa oportunidad y que ese talento que ahora se está dedicando a otras cosas se pueda utilizarlo tanto a nivel nacional como a nivel de empresa pública o privada.

Muchísimas gracias.

cve: DSCG-12-CM-126

El señor **PRESIDENTE:** Muchas gracias, señora Cabezas.
Tiene ahora la palabra el compareciente.

El señor **DE LA CUEVA GONZÁLEZ-COTERA** (abogado y doctor en Filosofía, profesor asociado de la Universidad Complutense de Madrid): Gracias, señor presidente.

Si se ha planteado alguna pregunta de manera duplicada, permítanme que responda de manera conjunta. Señor Salvador, el problema que usted ha apuntado es un problema que existe tanto en el *software* propietario como en el *software* libre, con lo cual la calidad o la naturaleza del *software* van a ser exactamente igual. El problema se resuelve de una manera muy clara, que es mediante la apertura de las API, que son los Application Programming Interface, es decir, el sistema de comunicación entre los distintos programas. Todavía queda por definir cómo tiene que ser la estructura de la arquitectura de la información en la sociedad digital que respete la separación de poderes, todavía no sabemos cómo tienen que ser esa redes, aún no ha habido un diseño, no ha habido un teórico que nos haya dicho: el principio de separación de poderes de Montesquieu, trasladado al siglo XXI y en el mundo de las redes, tiene que ser esta naturaleza para que independicemos la información que llega de un lado a otro. Siempre la tecnología ha ido por delante; cuando nacen los coches, no existe un código de circulación, por lo tanto, nos enfrentamos un problema que es universal, es un problema que es histórico, en el momento en el que surgen los microscopios, tampoco existe una legislación sobre cuáles son los centros que tienen que acceder a los microscopios electrónicos. La tecnología existe primero y posteriormente se produce su juridificación. La tecnología de la escritura en un determinado momento se utiliza para el derecho y el Tribunal Supremo recientemente, hace dos años, nos ha dicho cuáles son los tipos de fuentes tenemos que utilizar en los recursos contenciosos-administrativos, en definitiva, primero existe la tecnología y posteriormente la normativa sobre dicha tecnología.

Esto no significa —y utilizo aquí las palabras de Langdon Winner— que tengamos una política tecnológica. No, Langdon Winner lo que dice es que lo que existe es una ignorancia tecnológica en el sentido de que el legislador —la tecnología no es buena ni mala— todavía se cree que no es ni buena ni mala y no se ha dado cuenta de que la tecnología es política y que la tecnología tiene una política. Langdon Winner, en uno de sus libros, pone un ejemplo parecido a este: nosotros no podemos poner aquí, en la entrada del Congreso de los Diputados, un cartel que diga queda prohibida la entrada a las personas con discapacidad, pero lo que sí podemos poner es un escalón de un metro y medio, con lo cual, mediante la tecnología, ya estamos utilizando criterios para discriminar, y esto es lo que puede ocurrir, bajar de la teoría a la praxis.

Señor Salvador lo que está ocurriendo ahora mismo es lo que ocurrió con la codificación, exactamente igual. Se necesita un nuevo proceso codificador. Hace una serie de años se decidió realizar un código civil, un código mercantil, una ley de enjuiciamiento criminal y una ley de enjuiciamiento civil, se racionalizaron las diversas normas que existían. Me es igual si lo que tengo que racionalizar son diversas normas que están en cada uno de los supuestos, en cada uno de los sitios, si lo que tengo que hacer es producir estandarizaciones *de facto*, estandarizaciones que luego puedan ser utilizadas por todas las administraciones públicas y, a través de estas estandarizaciones, poder emitir de una manera muy práctica cuál es mi modelo semántico de datos. Lo que yo explico es qué modelo semántico de datos estoy dando. Por ejemplo, si la primera parte de este nombre es un nombre, si la segunda parte es el primer apellido y si la tercera parte es el segundo apellido. De esa manera puedo distinguir si la persona es norteamericana porque lo que va en medio es la segunda inicial de su nombre. Por tanto, mediante esos metadatos, si es norteamericano, yo ya sé que las dos primeras partes son nombre y si es español yo sé que esas dos segundas partes son apellidos. Por tanto, la web semántica, la semantización de la información que yo tengo que estar trasladando y con la que tengo que estar funcionando, esa categorización es precisamente esa nueva codificación que nosotros tenemos que hacer. La historia nos dice cómo se realizó la codificación francesa y esa actualmente la tenemos que hacer con este nuevo lenguaje formal. Entiendo que eso se puede hacer. Hay aplicaciones prácticas. Por ejemplo, la Administración pública española tiene el proyecto Afirma que está en GitHub. Ayer mismo se puso un comentario sobre si la utilización del Java 8, que está introducida en el código, es conveniente o no es conveniente y se está viendo y se están realizando aportaciones para que yo decida sobre mi Linux —porque yo solamente utilizo Linux, porque me apetece tocar el código fuente; lo siento mucho, no utilizo Windows porque no sé qué va a hacer ese ordenador conmigo— porque no me apetece que me ponga un icono de un juego XBox. No quiero que en un ordenador que es mío se me ponga un icono de Xbox; no juego con el ordenador, quiero decidir qué

cve: DSCG-12-CM-126

hay en el texto de mi ordenador, eso lo decido yo porque me lo he comprado y porque le he puesto el sistema operativo.

La aplicación @firma es un ejemplo perfecto de un buen uso y una buena manera de realizar las cuestiones por parte de las administraciones públicas y allí estamos los ciudadanos realizando determinado tipo de comentarios. Esto es absolutamente trasladable y es un modelo de gestión del trabajo, no es ni más ni menos que pongámonos a trabajar de una determinada manera. Cuando ustedes llegan aquí, las personas que son nuevas tienen que aprender cómo se hacen las enmiendas a una determinada normativa, saben que existe un determinado tipo de enmiendas y hay unas plantillas que se utilizan para hacerlas y el que viene de fuera lo primero que tiene que aprender es eso. Pues eso mismo es lo que hay que hacer precisamente con los lenguajes formales, establecer rutinas y procedimientos de trabajo y estas se tienen que extender. Lo primero que hago cuando mis alumnos llegan el primer día a clase, lamentablemente —y esto es en la Universidad—, es explicarles cómo tienen que ordenar los archivos del ordenador cuando me envíen los trabajos. En segundo lugar, que utilicen, por favor, *style sheets*, plantillas de estilo, para que cuando tenga que hacer un trabajo de veinticinco folios no tenga que seleccionar todo el texto de los veinticinco folios para modificar una fuente que luego les ha cambiado el título y, por tanto, tienen que emplear treinta horas en formatear un documento. Esto es lo esencial. Somos analfabetos digitales. ¡Cuidado!, no existen tampoco los nativos digitales; eso fue un invento del señor Prensky, que luego, afortunadamente, siete años después, se desdijo de lo que había dicho, pero ha hecho mucho mal con aquella afirmación. No existen los nativos digitales, como tampoco existen los nativos automovilísticos; todo eso son fanfarrias, fanfarrias que, por cierto, producen mucho dinero. Por tanto, estamos en esos sistemas en los que, con Fredric Jameson, tendríamos que decir: hablar de las cosas como si fueran nuevas lo que genera es mucho dinero. Si yo digo que esto es antiguo no me lo compra nadie. Siempre estamos con ese tipo de cuestiones. Señor Salvador, creo que le he respondido a sus preguntas y a sus inquietudes.

Respecto a la señora Angustia, yo también leí la discusión en Stack Overflow sobre si Python era o no el lenguaje preferido si tenemos que desarrollar o utilizar un determinado tipo de lenguaje de programación. Con los lenguajes de programación ocurre como con los lenguajes que se utilizan en la ciencia, la lengua vehicular. Por ejemplo, hoy, día 23 enero, también en un grupo de treinta y seis instituciones europeas —bueno, treinta y seis instituciones más una persona física, que soy yo— hemos ido a un *call* de la Unión Europea para el desarrollo de una aplicación que es Food Nutrition and Security para la European Open Science Cloud. Nosotros ahí llegamos con toda una serie de lenguajes de programación, y no nos olvidemos que el lenguaje de programación nos está permitido traducir una serie de datos en otros. El lenguaje de programación nos sirve para tomar una serie de datos, hacerles las transformaciones que sean necesarias y de ahí extraer los datos que necesitamos para otra cuestión. Mark Twain decía: 'Le envío a usted este documento en cuatro folios porque no he tenido tiempo de enviárselo en dos'. Los lenguajes de programación nos sirven precisamente para que en los momentos en los que nosotros tenemos una determinada necesidad de transformar una información —esos cuatro folios transformarlos en dos—, obtengamos la parte que es sustancial, que es elemental o sintética de esos datos que nosotros necesitamos, y en ese proyecto estamos utilizando muchos lenguajes de programación. No tenemos ningún tipo de problema con el lenguaje de programación. Podemos hacer ciencia en inglés —evidentemente allí estamos vertebrando todas las comunicaciones en inglés—, pero de repente, en un momento determinado, un subgrupo también lo puede hacer en alemán. El problema luego son las traducciones que puedan existir entre los distintos sistemas. Sí que es verdad que luego las comunidades de *software* desarrollan lo que son las librerías o las aplicaciones para ese tipo de utilización, y es verdad que cuando estamos hablando de *big data* Python tiene una ventaja porque tiene una aplicación que se llama Pandas, que es la que mejor ha sido diseñada precisamente para la trasformación de la información que nosotros tenemos que hacer. ¡Cuidado!, aquí tenemos que hacer una advertencia, el problema del *big data* es tan antiguo como que hace 2500 años un grupo de griegos se planteó que tenemos un exceso de información en el mundo y no sabemos cómo procesarlo y nació la filosofía y de la filosofía luego nació la ciencia, se desgajó la ciencia. Por tanto, el problema del *big data* no es nuevo, tiene 2500 años, pero en aquellos momentos la herramienta que se utilizó para procesarlo fue la racionalización, pasamos del mito al logos, y ese logos fue la herramienta que sería el equivalente a lo que hoy en día son los lenguajes de programación con los que nosotros estructuramos. La verdadera dificultad de saber qué tipo de información es la que yo tengo que obtener o utilizar aquí, porque, si no, me voy a la realización de determinados tipos de conexiones y veo conexiones en todos lados —en ocasiones veo conexiones—; entonces resulta que

cve: DSCG-12-CM-126

aquí he obtenido un determinado tipo de información que si cruzó con otra obtengo una serie de premisas, y ahí nos vamos única y exclusivamente a la limitación de lo que puede ser la argumentación. Por tanto, ahí nos volvemos a cuestiones de tipo clásico y vamos al mundo de los sofismas. Por ello, el mundo de los sofismas es previo y es necesario, y el algoritmo lo que nos oculta muchas veces es la capacidad que nosotros tenemos de analizar cómo se está pensando y de esa manera no podemos evitar la utilización de una determinada manera ilógica de proceder.

En cuanto a cuál es el sistema más seguro y que tiene más recursos de futuro, pasa igual que con las lenguas. Hace sesenta años en este país había que aprender francés, posteriormente se vio que había que aprender inglés y hoy en día hay que aprender chino. Yo soy partidario de aprender alemán, entre otras cosas por la deriva que está teniendo Europa. Evidentemente, al final hay que saber cuantos más idiomas mejor. Es cierto que precisamente son las comunidades de usuarios las que van a imponer determinados tipos de maneras o de tendencias. También hay que tener mucho cuidado con las tendencias porque muchas veces son modas pasajeras. Por tanto, una capacidad crítica para poder predecir muchas veces es muy difícil, es decir, tenemos esas limitaciones epistemológicas.

Sobre docencia, formación y mejorar la formación superior, le voy a contestar al mismo tiempo a la señora Cabezas y a usted. Yo ya he manifestado que lo que necesitamos es un grado no en ciberseguridad, sino un grado donde confluyan tres tipos de disciplinas que actualmente existen. En primer lugar, la disciplina de la documentación y biblioteconomía. Lo que estamos haciendo es categorizando y catalogando, y no nos olvidemos de que categorizar significa invisibilizar. Cuando yo hago categorías, aquello que no categorizo lo estoy dejando fuera y, por tanto, lo estoy haciendo invisible. Así pues, le puedo estar aplicando determinado tipo de problemáticas en las cuales yo genere luego injusticias precisamente por cuestiones de desigualdad. En estos estudios tienen que converger, en primer lugar, la documentación y la biblioteconomía; en segundo lugar, la informática y, en tercer lugar, el derecho, porque nosotros lo que necesitamos son especialistas jurídicos que sepan leer código fuente y que sepan todo lo relativo a la administración de documentación y a la gestión de la información; y esa nueva manera de ver las cosas no existe. Nosotros necesitamos un abogado del Estado que nos pueda decir: sí, estoy de acuerdo con que la administración de la Administración de Justicia sea del Ejecutivo, pero es que ya no estamos hablando, como decía David Maeztu, de máquinas de escribir; es que estamos hablando de un ordenador, y en este ordenador la administración de la Administración de Justicia no tiene por qué tener ningún tipo de competencia sobre lo que hay en el papel, o sea, en el disco duro, porque el soporte digital es el papel del siglo XXI, y este soporte digital está secuestrado y tiene una póliza en favor de las entidades de gestión en virtud de la compensación por copia privada. Y también tenemos que tener muy claro si no nos están invadiendo competencias a la seguridad del Estado o a las aportaciones del Estado. Nosotros tuvimos un periodo de diez años en el que por cada juicio que se celebraba en España, en aplicación de los artículos 147 y 187 de la Ley de Enjuiciamiento Civil, las entidades de gestión se llevaban 20 céntimos de canon sobre el CD. Afortunadamente, luego vino el Tribunal de Justicia de la Unión Europea y nos dijo que esto era absolutamente irregular y contrario a la directiva europea. Por tanto, lo que se nos plantean es ese tipo de problemas. El abogado del Estado tiene que tener la capacidad suficiente como para decirle a cualquier órgano del Estado: ¡Pero qué hace usted aceptando las condiciones de Twitter! Porque sabe de la existencia de las licencias mediante *click*, porque conoce precisamente cómo funcionan las redes. Y siempre estamos con la misma pregunta, y perdónenme ustedes que la critique porque es errónea: ¿Es que el abogado tiene que saber programar? Esa pregunta es errónea; el abogado no es que tenga que saber programar o no, tiene que saber algo más que programar. Porque dentro del mundo de la informática hay dos perfiles muy grandes y muy definidos, que son el del programador, el que escribe textos formales que luego se transforman en un código binario y se compilan para que se ejecuten en máquinas, y el que diseña redes. La ciberseguridad es diseño de redes, pero hay un componente esencial y es en qué tipo de programas yo estoy ejecutando dentro de redes, porque cuando se produce determinada intrusión puede producirse desde dentro porque se ha instalado un troyano, y ese troyano está programado. El abogado del Estado del siglo XXII tiene que ser una convergencia entre estos tres tipos de saberes: documentación, informática y derecho. No se puede ya separar de una manera tan evidente lo que es la norma jurídica simplemente porque esté escrita en un texto natural que todos entendamos. La norma jurídica se está ejecutando desde sistemas aplicativos, que son los que nos generan derechos y obligaciones; obligaciones también en el sentido que nos ha manifestado la señora Cabezas.

En cuanto a qué es necesario adoptar y qué tipo de formación de la Administración pública se puede mejorar, evidentemente hay que dotar a nuestros funcionarios públicos de ese tipo de conocimientos, no

cve: DSCG-12-CM-126

todos, obviamente, pero sí los elementos estructurales, aquellas personas que estratégicamente sean las responsables tienen que conocer perfectamente cómo funciona el sistema, cómo funcionan las tripas del sistema. El burócrata weberiano, que era el que finalmente se hacía con el poder, hoy en día tiene una significación totalmente distinta y es una persona que, además, conoce perfectamente cómo ha de configurarse una red, por qué tenemos que aceptar una configuración que nos viene impuesta desde fuera porque ya en ese aspecto estamos en la parte pragmática y no nos permiten utilizar el sistema sintáctico y, por tanto, crear los mundos que nosotros creemos.

Respecto a canalizar el talento —uno esto con la señora Cabezas—, esa es la gran pregunta de este país: por qué todos mis amigos brillantes están fuera de España. No es un problema de ciberseguridad, es un problema de este país. Somos pioneros en dos grandes tecnologías: fútbol y restauración, y a mí me gustaría que fuéramos pioneros en muchas más tecnologías. Agradezco que mis amigos estén fuera de España porque hago viajes a sus casas y siempre es un placer visitarles, pero me parece que necesitamos una reflexión. Tuve el honor de asistir aquí también cuando se solicitó una nueva ley de la ciencia por parte del presidente de la CRUE y con intervención de la señora presidenta, y entiendo que ese es el camino por el que hay que ir: se requiere y se necesita una nueva ley de la ciencia y que el presupuesto en ciencia y tecnología se eleve simplemente a los niveles estandarizados de los países desarrollados. No se puede hacer ciencia y tecnología cuando lo que nosotros estamos haciendo, el talento, no se puede canalizar sin un requisito previo que es una dotación presupuestaria. No puede hacerse una Ley contra la violencia de género sin dotación presupuestaria; el dinero es fundamental y, por tanto, para que podamos hacer algo sobre el talento necesitamos una dotación presupuestaria, y ahí es donde hay que incidir.

En cuanto a *hackers y crackers*, evidentemente, lo mediático ha hecho que entendamos por *hachers* lo que en su momento eran los *crackers*. Un *hacker*, desde un punto de vista canónico, es una persona que da una respuesta brillante a una pregunta inteligente. El doctor Barnard fue un *hacker* del corazón. Posteriormente, los medios fueron variando el contenido semántico. No podemos evitar que las palabras, según el tiempo en el que existan, vayan cambiando de su continente a su contenido y lo vayan modificando semánticamente. Hoy en día *hacker* es aquella persona mala que entra en los ordenadores y que normalmente está en casa metido con un gorro de invierno; así nos lo expresa la publicidad.

Respecto al problema de Lexnet, en mi opinión, el diseño de Lexnet responde a esa primera pregunta de cómo tiene que ser la arquitectura de las redes cuando estamos en una sociedad que respeta la división de poderes de Montesquieu. Mis datos no tienen por qué salir del juzgado donde yo estoy llevando el asunto. Por tanto, es el juzgado el único que tiene que tener la capacidad de tener eso. El Poder Judicial es quien tiene que administrar Lexnet y no puede ser que una Consejería de Justicia de una competencia delegada tenga el control sobre los juicios que se están realizando contra el propio consejero por una cuestión de corrupción. Esto es ilógico y es lo que está ocurriendo ahora: el consejero de Justicia de una comunidad autónoma tiene acceso a los procedimientos judiciales de su comunidad autónoma. ¿Lo hemos pensado bien? El problema de Lexnet es que cuando antes yo presentaba una demanda en papel la presentaba abajo, en mi juzgado, y era el juzgado el que decidía dónde iba la información, si iba al Registro Civil, si iba al Registro de Penados; si es un matrimonio va al Registro Civil, si es un fallecimiento, etcétera. Hay que volver a tener eso y es lo que volvemos a necesitar.

Respecto a lo que ha dicho el señor Luena de si vamos a ser manejados por los datos o vamos a ser nosotros quienes los manejemos, vuelvo a hace 2500 años, exactamente igual, el mismo problema que se está produciendo ahí también lo tenemos en las sociedades ágrafas y con el analfabetismo, con lo cual lo que nos está señalando este autor es algo ya conocido. No olvidemos que Felipe II tenía dos tipos de asesores: en primer lugar, tenía a los hombres de armas y, en segundo lugar, a los hombres de letras y, de los hombres de letras, vienen los letrados y de ahí que cuando yo voy a un juicio me digan el letrado señor De la Cueva. Ciertamente, al final están las grandes corporaciones, pero por ejemplo en FNS Cloud somos un consorcio público-privado y actualmente tenemos que tener en cuenta que existe una enciclopedia universal que se llama Wikipedia y que en el año 2002 cuatro personas en España nos enfrentamos a Jimmy Wales y le dijimos que así no tenían que ser las cosas. Le dijimos: a partir de este momento usted tiene que interponer una fundación, no puede ser una corporación privada la que, mediante publicidad, se haga propietaria de nuestros datos. Eso ha ocurrido en Facebook, ha ocurrido en Twitter, pero lo evitamos cuatro españoles en Wikipedia con la intervención de la Universidad de Sevilla. Vamos a ver, actualmente —por utilizar una palabra de Bruno Latour— existe el concepto de ensamblaje. La Wikipedia tiene los textos que vamos escribiendo personas privadas. Estos textos privados los donamos, donamos nuestro

cve: DSCG-12-CM-126

conocimiento a la humanidad y formamos lo que es un procomún digital. Este procomún digital es de todos pero no es de nadie y todo el mundo puede hacerse propietario de ello pero nadie puede excluir a los demás, con lo cual no coincide con la exactitud del concepto del dominio que deriva del Derecho Romano ni el que tenemos en nuestro Código Civil. Al mismo tiempo, también va por cables, que son privados, y luego los procesadores que gestionan esos ordenadores también son privados y además hay satélites que son públicos. Por tanto, el nuevo modelo de mundo que estamos construyendo tiene un ensamblaje de un procomún digital de corporaciones privadas y de actores de tipo público. El problema es de gobernanza y de cómo logramos —y así lo hacía saber la doctora Nadal en su momento— el equilibrio entre los requisitos de la sociedad, los requisitos de las corporaciones, los requisitos de los usuarios y los requisitos políticos. Es un problema, por tanto, de gobernanza y de sostenibilidad, que es sobre lo que la Unión Europea está tan absolutamente preocupada en su nueva European Open Science Cloud.

¿Impuestos, multas? Por supuesto, por supuesto, absolutamente, pero el problema es que tenemos que definir y trasladar un sistema de impuestos que estaba diseñado para sistemas inmobiliarios de construcción de inmuebles, con lo cual tú tenías muy claro dónde radicaba la información y la actividad, que era en el lugar donde construías y ahí era donde se realizaba el hecho imponible, a los sistemas actuales a los que tenemos que empezar a trasladar qué datos estoy obteniendo: si estoy obteniendo los datos de un nacional de aquí, entonces el beneficio se está obteniendo con un nacional de aquí y usted tiene que pagar impuestos aquí. Ese traslado de impuestos, ese traslado del lugar del hecho imponible es en el que sé que actualmente algunos especialistas fiscales están trabajando a nivel de la Unión Europea.

Respecto a mi opinión sobre la Directiva de ciberseguridad, me parece un magnífico comienzo pero, como siempre, *learning by doing*, aprendemos haciendo, y estamos en una fase determinada y no olvidemos que en 1440, aproximadamente, es cuando se inventa la imprenta y los grandes efectos de la imprenta los tenemos obviamente en la reforma protestante y, los grandísimos efectos de la imprenta, los tenemos en 1676 y 1789, y estoy hablando de las revoluciones que luego conducen a la implantación de los derechos fundamentales. Las instituciones por fin acogen aquellas ideas, en palabras de Bobbio. ¿En qué puesto nos hallamos? Nos hallamos en un buen puesto. No me gustan nada las listas porque vivimos en una sociedad demasiado numérica, todo está numerizado: va usted al Corte Inglés y tiene que decir si le ha gustado o no, sale usted de un cuarto de baño y tiene que decir si la función ha sido buena o no. No quiero poner números, y me voy a Platón: La verdad, la bondad y la belleza no son mensurables; la justicia no es mensurable; los grandes valores no son mensurables. Ese es el gran problema que tienen las métricas y existe una imposibilidad de valorar determinado tipo de cuestiones que son precisamente las que nosotros tenemos que implementar. Podemos hacer determinado tipo de métricas de la justicia, pero la justicia considerada en sí misma es anumérica y, por tanto, respecto a la lista en la que estamos, el problema que a lo mejor tenemos es que precisamente en la ciberseguridad —muchos amigos que se dedican a este tema me lo comentan— su labor siempre es callada y oculta; nunca se ve que lo hacen bien, porque solamente se ve que lo han hecho mal cuando se produce una intrusión. Entonces, si no ha pasado nada, ¿lo han hecho bien, lo han hecho mal o es que no ha venido nadie? Si la policía en la frontera no incauta cocaína, ¿lo está haciendo bien o lo está haciendo mal? ¿Significa eso que no lo está haciendo bien? Se puede decir que sí pasaría cocaína, pero también puede ser que no. Ese es el problema de la *probatio diabolica* y aquí es precisamente lo que tenemos.

En relación con la coordinación con el sector privado y la estructura, nivel de política comparada, creo que se están haciendo muy bien las cosas. Creo que existen suficientes ejemplos en las intervenciones que se han hecho aquí. Hubo una ponente, diplomática, Julia del Olmo, que explicaba cómo era la estructura. Me parece muy bien. ¡Cuidado!, como siempre, detrás están las personas y, al final, resulta que una gran estructura organizacional puede funcionar muy bien pero luego hay un conflicto interpersonal entre dos personas que están allí por cualquier tipo de cuestión y entonces ya no importa el diseño que nosotros hagamos porque si la relación entre ambas personas no tiene ningún tipo de simpatía entonces lo que hacemos es eludirlo. Sobre simpatías políticas, creo que este es el mejor sitio como para saber que existe también ese tipo de cuestiones.

Me ha preguntado usted también sobre fortalezas y vulnerabilidades. El problema de la vulnerabilidad es lo de siempre, que no se ve hasta que ocurre, con lo cual es muy difícil realizar este tipo de vulnerabilidad. Sí que es verdad que existen actualmente tecnologías para trabajar continuamente en estas fortalezas. Sí que hay una cuestión que me parece bastante relevante, que es la siguiente, el *software* libre no tiene departamento de corrupción. El *softwar*e libre no puede invitar a nadie a cenar, no puede pagar vacaciones a nadie, no puede montar congresos. Por tanto, el *software* libre nunca podrá

cve: DSCG-12-CM-126

implantar sus soluciones más que desde una parcela teórica, en el sentido de mostrar sus bondades. El *software* libre entiendo que muestra sus bondades. Por tanto, un problema de fortaleza que puede existir aquí es la desventaja comercial existente entre dos soluciones, que siempre la del *software* libre puede ser mejor porque tiene mejores demostraciones, pero no hay nadie que alce la voz, no hay comerciales, simplemente hay técnicos; y, como se dice en el mundo académico, o te vendes o trabajas. Con lo cual, vas a descubrir que un buen académico es bueno porque a lo mejor no le conoces más que a través de su obra, y no a través de sus apariencias en determinado tipo de eventos.

Estoy totalmente de acuerdo con mi compañero David Maeztu en cuanto a las administraciones públicas y los ayuntamientos. Hay una carencia de formación brutal; y no solamente hay una carencia de formación brutal, hay una carencia de recursos brutal, una carencia espectacular, y hay una carencia de coordinación brutal. Necesitamos sistemas de apoyo para todas las administraciones públicas. Pero volvemos un poco a lo mismo, si en 1440 nace la imprenta, los efectos de la imprenta los vemos en 1789. Pues aquí pasa exactamente igual, no nos olvidemos de que es una tecnología que tiene veinte años; es en 1993 o 1994 cuando empieza el *boom* de Internet, de la web en España, no de Internet; Internet podemos irnos a 1960. El periodo que hemos realizado que tenemos hasta ahora es muy corto y, aparte, tiene otro problema, que es que desde el momento en que la tecnología lo que hace es eludir o esconder lo que hay, y te lo da con una cierta apariencia, parece magia. De esa manera, nos encontramos con la imposibilidad de verificar qué es lo que está ocurriendo detrás. Por ejemplo, voy a un restaurante y digo: ¿La hamburguesa puede ser sin mayonesa? Y me dicen: No. Bien, no puedo operar en la capa pragmática; me obligan a tener todo un bloque. Y esto es lo que está ocurriendo, te obligo a tener todo un bloque, toda una serie de paquetes. Oiga, yo no quiero en este paquete un paquete de presentaciones porque no lo voy a utilizar. Esto es lo que está ocurriendo dentro de las administraciones públicas.

En cuanto a la evolución presupuestaria, más dinero, se requiere más dinero. En relación con los cibervoluntarios y su regulación, Colombia, efectivamente, nos da un maravilloso ejemplo. Aquí volvemos a introducirnos en un problema de formación. Nosotros estamos acostumbrados a la formación en sistemas formalizados. El *hacker* siempre ha aprendido en sistemas informales. Todo lo que yo sé de seguridad, todo lo que yo sé de ordenadores, lo aprendí en un grupo de *hackers* absolutamente maravilloso, a los cuales les doy un homenaje desde aquí, que se llamaban Escomposlinux, y los cuales por supuesto figuran en mis agradecimientos de mi tesis doctoral. El aprendizaje informal que yo realice ahí no se tiene en ningún tipo de universidad. Hay maestros que nos enseñan verdaderas maravillas. Las personas que están en hostelería y puedan tener varias estrellas Michelín, muchos de ellos sí que han ido a lugares de hostelería para aprender, pero muchos lo han hecho en casa y mediante tradiciones familiares. Esto existe también dentro de las comunidades. Se produce lo que se ha venido a denominar por parte de académicos de Harvard a partir de 1990, Wenger y siguientes, las comunidades de prácticas, las comunidades de aprendizaje. Y el gran reto que tienen las universidades actualmente es cómo incluir dentro de sus formaciones o cómo modelar sistemas de aprendizaje como el que se realiza, por ejemplo, en Medialab-Prado en Madrid, que siempre ha sido un homenaje, y donde a partir de 2007 tuvimos el Laboratorio del Procomún, donde también aprendimos muchísimos de estos conceptos sobre los que nunca, en ninguna universidad, ha existido ningún plan de estudios. La universidad va por detrás de estas comunidades de aprendizaje.

En cuanto a formación en seguridad, efectivamente, se requiere dentro de ese grado, por supuesto, que yo propongo. En relación con la carta específica de derechos y deberes digitales, no puedo estar de acuerdo. Los derechos y deberes digitales están dentro de los derechos y deberes fundamentales, y luego ya veremos. ¿Qué hacemos? ¿Una carta específica de derechos y deberes del automovilista? Bueno, pues es código de circulación; entonces, ya no es de derechos fundamentales. 'No atropelle usted'; bien, pero es que eso ya está en el derecho a la vida; o 'no vaya usted siendo un kamikaze'; bien, pero ahí ya estamos en delitos de riesgo.

En cuanto a las injerencias que pudo haber en la política nacional en la crisis catalana, lo que yo siempre me planteo, cuando leo este tipo de cosas, es si no es más venenoso para una sociedad el sistema de televisión privada que tenemos y los contenidos a los cuales accedemos, que cualquier influencia de los —comillas— «*hackers*» —comillas— «rusos». Y no quiero citar a nadie en el mundo de las tripas, pero se me ocurren unas cuantas personas que están en boca de todos. Eso sí que a mí me parece un ataque a la democracia, porque nos impide ser ciudadanos críticos. El nivel de entontecimiento al cual han llegado los medios de comunicación es tan brutal, que cuando alguien me dice que hay *fake news*, o leo que el señor Cebrián lo que hace es criticar las *fake news*, digo: ¡Caramba!, voy a buscar

cve: DSCG-12-CM-126

aquella cita donde se decía que la editorial de *El País* lo que lograba era cambiar la opinión de Miguel Boyer en un Consejo de Ministros. Con lo cual, dónde nos vamos; nos vamos a una reflexión crítica de lo que es la sociedad y de lo que son los medios de comunicación, y el problema que tenemos es un problema epistemológico; es un problema de dónde puedo beber, qué fuentes pudo tener para ser un ciudadano informado de una manera correcta. Y lo siento, los medios de comunicación de hoy en día no nos dan esa posibilidad, no nos la dan. Por lo tanto, el problema es mucho más grave que una mera cuestión de lo que pudiera existir de los *hackers*, de los *crackers* rusos con respecto a la crisis catalana. ¿Alguien se puede creer de verdad que el Papa Francisco lo que hizo fue apoyar a Trump? Miren ustedes, hay veces que uno lee *El Mundo Today*, del cual yo soy fan, y uno no sabe si es verdad o es mentira. Pero es que hay veces que uno lee noticias en otros periódicos y dice: ¡Esto es de *El MundoToday!*, y resulta que ha sido verdad! Esto es lo que nos podemos encontrar. Con esto espero haber respondido a todas sus preguntas y no haberme dejado ninguna de ellas.

A la señora Cabezas quería decirle que no tenemos seguridad al cien por cien al cruzar la calle, eso es evidente. La sociedad del riesgo del señor Beck es una sociedad en la que nosotros vivimos. Y con respecto a su apreciación de que las tecnologías son demasiado rápidas, yo creo que es un problema de plantearnos simplemente cuál es el enfoque que nosotros tenemos. Vamos a ver, si yo miro dentro de un árbol, veo que las hojas se mueven continuamente. Sin embargo, si yo ese árbol lo veo a 20 o a 10 kilómetros de distancia está inmóvil. A las tecnologías de la comunicación y de la información les pasa exactamente igual. Desde fuera parece que están continuamente moviéndose, pero no han variado desde 1960, 1970, donde lo que se hizo fue el TCP/IP. Lo que varía es la moda; lo que varía es el traje; ¿qué traje me pongo hoy? Siempre me pongo una chaqueta y corbata, pero es distinta. Entonces, ¿dónde analizo el cambio? Si el cambio lo analizo estructuralmente no hay ningún cambio; si el cambio lo analizo desde una manera superficial, efectivamente, cada dos por tres hay actualizaciones, hay programas. Vino la *tablet* y continuamente, no nos olvidemos, estamos en el mundo de generar necesidades que no tenemos para que compremos cosas y sacarnos el dinero. Esta es la sociedad en la que nosotros vivimos actualmente; es la sociedad del espectáculo, porque el resto del dinero que te sobra te lo voy a obtener entreteniéndote. Entonces, una vez que tienes gastado esto, te voy a sacar esto otro para que, al final del mes, no te quede absolutamente nada. La única diferencia entre ganar 2000 o 4000 es el número de veces que vas al cajero automático, como decía un amigo mío.

¿Qué es lo que nosotros tenemos que reflexionar con respecto a la tecnología? Nosotros hacemos exactamente la misma función con el ordenador que la que hacíamos hace veinte años: escribir textos, ver videos y hacer hojas de cálculo. Otra cosa son los ingenieros o arquitectos o los que son realizadores de video que necesitan una mayor agilidad, pero los demás hacemos exactamente lo mismo. ¿Cuántos ordenadores hemos tenido que comprar y cuantas actualizaciones hemos tenido que sufrir? Cuántas veces hemos oído eso de: te pongo una actualización y entonces ya no me llega el ordenador, me tengo que comprar otro, me pongo otra actualización. Mis ordenadores tienen quince años, funcionan con *software* libre y no tengo ningún tipo de problema con ellos. ¿Por qué? Porque como jurista me dedico a estudiar, leer y hacer textos. Entonces, todas aquellas funciones que sean de esa naturaleza no hubieran tenido jamás que haber generado un ecosistema de basura tan grande como el que nosotros hemos generado con el mundo de los ordenadores. Los problemas que derivan de esta aceleración en el consumo son gravísimos. Por tanto, yo niego la mayor en el sentido de que vayamos cada día más rápido. Sí, en el número de trajes que nos ponemos, pero siempre llevamos traje y siempre llevamos corbata. Esto no cambia desde hace muchos años.

Efectivamente, estoy totalmente de acuerdo con usted, ha de ser una política de Estado como las grandes políticas de Estado; no puede ser, es una cuestión de soberanía tecnológica. El control sobre el código fuente, el control sobre qué tipo de legislación puedo hacer y, por tanto, qué tipo de *software* tengo que hacer es una política de Estado mayor, y es una política de Estado mayor porque precisamente a través de eso se producen los grandes riesgos del Estado: que no funcione Barajas, que no pueda eludir una agresión, que no pueda tener acceso a unas condiciones de tipo bancario, que se paralice la Administración pública. Todo este tipo de recursos son estratégicos y, por lo tanto, se requiere una alta política de Estado sobre ese tema y unos funcionarios absolutamente formados en esta alta política del Estado, con este cuerpo de funcionarios en esos tres conocimientos.

La valoración —voy acabando— desde que empezó Internet sobre en qué hemos avanzado y dónde estamos fallando es que hemos pasado de una promesa de la sociedad del conocimiento a una sociedad de control. Ahí es donde nosotros estamos fallando. La pregunta que les haría a sus señorías es cuántos

cve: DSCG-12-CM-126

de ustedes tienen inhabilitada la ubicación en su móvil, porque estoy convencido de que la mayor parte de ustedes tienen la ubicación de su móvil cumplimentada. Ustedes son representantes del pueblo español, ¿cómo permiten que empresas extranjeras sepan dónde están ustedes en cada momento? Estamos como en los mejores tiempos de la Stasi. En su momento escribí un artículo donde decía —y me van ustedes a permitir la expresión— que esto es el sueño húmedo de Goebbels. Goebbels jamás fue dotado de unas herramientas de control tan magníficas como las del sistema actual de control que tenemos en esta sociedad, a las que nos hemos sometido libre y voluntariamente. Decimos que es mucho más cómodo porque así uno sabe en qué restaurante estuvo anteayer. Eso es lo que estamos haciendo. No nos olvidemos de que la tecnología no es algo de lo que podamos escapar. No, somos nosotros quienes tenemos que diseñar las tecnologías. Es que si usted tiene un Roomba en su casa, un aspirador, sabe qué días está usted en casa y cuáles no y se lo da a una empresa. Y si usted en la cocina tiene un robot de cocina sabe qué comidas son las que usted hace porque lo envía, porque si no tiene wifi no se pueden actualizar las recetas. Esto está ocurriendo. Ponga un espía en su cocina, ponga un espía en su vida cotidiana y ponga un espía en su coche —obviamente— y ponga un espía en todo. ¿Dónde hemos llegado? Hemos pasado de la promesa de una sociedad de la información y del conocimiento a la existencia de una sociedad del control y este control no lo están ejerciendo los Estados, lo están ejerciendo otro tipo de poderes.

Educación para las tecnologías, por supuesto. Desde el momento en que tenemos habilitada la ubicación de nuestro móvil es que tenemos que empezar desde lo más básico, desde el abecé de la tecnología. Tenemos que saber que tenemos unos aparatitos diabólicos y estos aparatos diabólicos a través de la triangulación de antenas —aunque no tengamos la ubicación— saben exactamente dónde estamos. Y eso está en manos de empresas teleoperadoras. Afortunadamente, la Unión Europea anuló la directiva por la cual se permitía que tuvieran estos datos almacenados para siempre por una cuestión de seguridad. Cuidado también con la seguridad, porque en nombre de la seguridad cuando uno entra en una autopista se le comunica que 'por su seguridad le vamos a grabar', 'esta conversación se puede grabar por su seguridad'. Oiga, no, tengo suficiente inteligencia para saber que usted me está diciendo seguridad cuando usted se refiere a que le viene muy bien grabar eso porque ya verá usted qué hace con ello. Eso es lo que nosotros tenemos.

Sobre los 100 000 voluntarios de ciberseguridad en Colombia, estoy totalmente de acuerdo. Me parece magnífico, creo que hay que promover siempre una visión de no precarizar la sociedad. Porque, por ejemplo, en esta Cámara se ha aprobado de una manera unánime el estatuto del artista, pero simplemente es una declaración, hay que trasladarlo a normas jurídicas. Cumplo hoy treinta años como abogado y me honro por ello y les doy las gracias por esta intervención, pero, señorías, no saben ustedes lo que ha sido ser treinta años autónomo, no se lo aconsejo a ustedes. Es una heroicidad ser treinta años autónomo, es muy complicado, los bancos no te apoyan, no te apoya absolutamente nadie. No entraré en ese tema porque no es este el objeto de esta comparecencia pero tenía también que decirlo.

Por último, hablaré del mundo de la infancia. En el mundo de la infancia hay un problema grave de educación y es que desde el momento en el cual el diseño de las aplicaciones informáticas no nos permite entrar en la configuración y nos la dan ya hecha —tenemos esta ocultación que parece magia, se produce ese *black box*, una caja negra en la cual no puedo saber qué se está haciendo dentro. Las personas de Canadá que tienen tractores resulta que tienen que cambiar el *software* porque el tractor no les permite hacer determinado tipo de acciones y el *software* les viene vendido con el tractor. Cuidado a ver qué va a ocurrir con el coche autónomo, porque nos van a imponer un determinado tipo de conducción y no nos van a permitir entrar en la configuración. Hemos visto también un problema de un avión que cayó en el Índico hace del orden de un mes y medio o dos meses, los informes dicen que se produjo un problema de *software*, manualmente no pudieron acceder. El ordenador del avión tenía un sensor mal en la cola y le fue dando mediciones distintas, por lo cual el avión por tres veces se puso prácticamente hacia abajo y al final se fue al mar provocando la muerte de todos los pasajeros. El piloto antes pilotaba manualmente, el piloto ahora no pilota, pilota un *software* a cuyo código no se tiene acceso y cuyo cambio entre el código y lo manual no es posible por un sistema de diseño. Por tanto, tenemos que reivindicar el control sobre la tecnología. Ese control sobre la tecnología solo se puede hacer a nivel sintáctico, no se puede hacer a nivel semántico. No se debe permitir que nos lo impongan a nivel semántico o a nivel pragmático. La soberanía tecnológica depende de que nosotros seamos capaces de vertebrar las combinaciones entre todos los distintos sistemas y signos que subyacen a esa tecnología. Y esto hay que educarlo desde el colegio, desde las familias, desde las escuelas y hay que hacer también un plan nacional de educación en

cve: DSCG-12-CM-126

este tipo de temas. Primer problema: reinos de taifas y eso es algo con lo que nos encontraremos, diversos tipos de implementaciones. Y el segundo problema es el problema presupuestario que afronta.

Señorías, espero haber sido capaz de responder a todas sus preguntas.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias. Señor De la Cueva, lo va a comprobar usted inmediatamente porque voy a dar turno a los portavoces para que le pregunten aquellas cuestiones que, en su opinión, no hayan sido contestadas.

Señor Salvador.

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

En primer lugar, independientemente de que pueda estar de acuerdo con muchos puntos de su intervención al margen de la ciberseguridad —porque su intervención finalmente ha terminado siendo muy poquito sobre ciberseguridad y más sobre el mundo tecnológico y lo que nos afecta a los ciudadanos en el día a día—, perdóneme que le diga que no me ha bajado a la praxis las propuestas concretas sobre ciberseguridad para poder trasladar su discurso teórico a esa parcela. Por otra parte, es verdad —repito— que cuando se hace un análisis del mundo y un discurso crítico es muy fácil coincidir en muchas cuestiones y muchos podemos estar absolutamente de acuerdo, por ejemplo, en el tema de la influencia y el peso que van a tener las corporaciones por encima de los Estados, de cómo la tecnología y el código son elementos fundamentales en el que se va a mover nuestra sociedad en todos los ámbitos y el que tiene ese control y capacidad de garantizar lo que él quiere es ser capaz de imponer a los demás muchas cosas y poder gobernar el mundo. En todo ese tipo de concepto teórico-realista podemos estar de acuerdo, pero también es verdad que al final no estoy de acuerdo con montones de los temas que usted ha tratado, simplemente, porque tenemos puntos de vista distintos, independientemente de converger en el fondo de la cuestión. Entiendo que usted sea un defensor a ultranza del *software* libre frente al *software* propietario, lo puedo entender. Yo utilizo Windows y no tengo ningún problema. Usted ha dicho antes que es abogado y no necesita que le ofrezcan mil funciones más si las tres que utiliza las puede mantener durante quince, veinte o treinta años. Pues yo también, todo lo que necesito de un procesador de textos, de una hoja de cálculo me lo da alguien que además me lo hace compatible con otro montón de aplicaciones que también utilizo y me permite funcionar mejor. ¿Por tanto, qué es mejor? ¿Lo uno o lo otro? Ni lo uno ni lo otro, la libertad de la persona de poder elegir si quiere utilizar *software* libre o *software* propietario. Le pregunto: ¿Una persona por utilizar *software* libre es más libre? ¿Todos los usuarios que utilizan *software* saben utilizar el código abierto y saben tocarlo? ¿O tienen un amigo al lado que sí sabe y se lo toca y consigue que le pase la información al amigo por las noches en vez de pasárselo a una multinacional? Todo eso es relativo. Una cosa distinta —y estamos hablando en una Comisión de ciberseguridad y Seguridad Nacional— es que usted me hubiera dicho que los gobiernos no tienen que utilizar código cerrado sin conocer su contenido y certificar que ese contenido tiene todas las garantías para que no pueda hacerse un uso contrario al objetivo que tiene ese país de proteger su información. Eso yo lo puedo compartir. Por tanto, que el código esté abierto en un momento determinado para que los Estados puedan verificar la información que hay dentro, que sepan que ahí no hay una compañía de telefonía china o coreana que se está llevando tu información, me parece bien. Otra cosa distinta es la filosofía de que todo el *software* de la Administración tiene que estar en código abierto o no puede estar en código cerrado. La cuestión es quién cierra el código y quién certifica que lo que hay dentro es correcto y está bien.

Un simple matiz, yo sí creo que hay nativos digitales. El diccionario dice que nativo es el que ha nacido en el lugar del que se trata o que tiene relación con el lugar de nacimiento, que es innato o natural. Es una acepción. Probablemente, cuando se dijo que había nativos digitales esos no eran nativos digitales; hoy en día los niños son absolutamente nativos digitales. Pero, en cualquier caso, es una cuestión terminológica. Cuando dice que hay que hacer una nueva ley de la ciencia, la Ley de la Ciencia se hizo en 2008, la Ley de la Ciencia, la Tecnología y la Innovación; se incluyeron conceptos que la hicieron completa, porque esa ley sustituyó a la Ley de la Ciencia de 1986. Lo digo porque fui quien presentó la moción en el Senado que dio lugar a ello. Lo que hay que hacer es desarrollar esa ley y esos conceptos de ciencia, tecnología e innovación y todo lo que llevaba en ese desarrollo. Porque estoy de acuerdo con lo que usted ha dicho también de que las leyes tienen que tener presupuesto y después reglamentos que las desarrollen porque si no, no valen de nada.

En cuanto a las métricas yo estoy de acuerdo totalmente, son principios de la calidad. Lo digo porque lo que usted está diciendo está quedando aquí reflejado y yo también quiero que quede reflejada esta

cve: DSCG-12-CM-126

posición. ¿Dónde debe estar el derecho de las personas cuando le preguntan por una métrica, el contestar o no contestar? A mí no me invaden las métricas si yo no quiero contestar; ahora, yo puedo contestar y perfeccionar el sistema para que se adapte más a mí. Hasta lo del avión que ha dicho al final. Es verdad que se pudo caer un avión por *software,* pero también hubo un piloto que por manejarlo manualmente…

El señor **PRESIDENTE:** Señor Salvador, tenemos tres minutos y yo creo que usted está interviniendo a modo de debate y no a modo de pregunta.

El señor **SALVADOR GARCÍA:** No, termino ya, rápidamente.

El avión se pudo caer por *software,* pero también el *software* protege que muchos aviones no se caigan por una mala utilización. Un piloto también tiró el avión en Francia y lo hizo porque lo conducía manualmente y no hubo un *software* que le impidiera hacerlo. Por tanto, creo que en este sentido todo es relativo.

Estamos hablando de ciberseguridad y la ciberseguridad tiene que ver con que hay personas que no respetan los derechos de los demás, que buscan vulnerabilidades en los sistemas y que los utilizan para usos fraudulentos y para cometer delitos, y lo que tenemos que hacer es blindarnos frente a ellos, no un debate filosófico sobre si *software* libre, *software* propietario o qué dependientes somos de nuestro futuro, de nuestra información o si los Estados tienen más o menos poder, independientemente de que entiendo que eso también es muy importante.

Muchas gracias.

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

Tiene ahora la palabra la señora Angustia.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Tomo la palabra solo para agradecer al ponente, al señor De la Cueva, todas sus reflexiones, las aportaciones y las propuestas que nos ha hecho.

Muchas gracias.

El señor **PRESIDENTE:** Señor Luena.

El señor **LUENA LÓPEZ:** Sí, gracias. Dentro de los tres minutos y con cierta distensión, porque veo que el señor Salvador se ponía tenso **(el señor Salvador García: Tenso nunca, por favor),** traemos a los comparecientes para que nos ayuden, para que ofrezcan líneas de debate, que hay que compartir o no. Yo creo que los ponentes del grupo ya tendremos nuestra oportunidad. En todo caso, cuando usted hablaba… No sé que sueño ha dicho de Goebbels…

El señor **PRESIDENTE:** Un sueño húmedo, ha dicho.

El señor **LUENA LÓPEZ:** ¡Ah!, vale. Me acordaba yo —decía, por introducir elementos de ironía— de algún personaje que últimamente vemos con una visera tapándose la cara, que va con un periódico así. Yo digo: si este hombre hubiera sabido todas las cosas, no sé que hubiera sido del Estado español; si hubiera sabido todas las cosas que intentamos evitar que sepan señores que van con gorra y periódico como el que vemos y que no pienso ni nombrar. Le vuelvo a agradecer el debate que ha suscitado esta mañana.

Yo le preguntaba sobre la conciencia de riesgo y voy a aprovechar este segundo turno para concretar más la pregunta. Aquí ha habido altos mandos militares que nos han dicho claramente que estábamos expuestos a un ataque yihadista en las redes. No sé qué opinión tiene usted desde los conocimientos y las lecturas que ha hecho, que hemos visto que son muchas.

En relación con Rusia, que usted ha comparado con un periodista y con los medios de comunicación, yo le preguntaba —y he dicho la Federación Rusa— porque es un Estado el que utiliza herramientas, *fake news*, *bots,* para intervenir claramente en la política de un Estado. Y como nos ha dicho usted que había que aprender idiomas, concretamente el alemán, ya no sé si decirle *Danke* o decirle en ruso, que podría estar de moda en esta Comisión, *spasiva.*

El señor **PRESIDENTE:** Muy bien. Muchas gracias, señor Luena, por este alarde lingüístico.

La señora Cabezas tiene la palabra.

cve: DSCG-12-CM-126

La señora **CABEZAS REGAÑO:** Gracias, presidente.

Simplemente mi intervención, en nombre de mi grupo parlamentario, es para agradecer a don Javier de la Cueva su comparecencia, su intervención, porque creo que esta Comisión debe ser para aportar, para trabajar todos juntos, precisamente, en seguridad nacional. La ciberseguridad ahora mismo es la quinta dimensión, como se suele decir. A España se la puede atacar por mar, tierra, aire y, en este caso, a través de las redes sociales y todo lo que es Internet. Por lo tanto, le agradezco su comparecencia, sus aportaciones y sus respuestas que creo que han sido bastante claras e ilustrativas para todos nosotros. Muchísimas gracias por su intervención.

El señor **PRESIDENTE:** Gracias.

Tiene la palabra el señor De la Cueva para contestar a los comparecientes.

El señor **DE LA CUEVA GONZÁLEZ-COTERA** (abogado y doctor en Filosofía, profesor asociado de la Universidad Complutense de Madrid): Gracias, señor presidente.

Simplemente quiero dejar claro algo que quizá no haya quedado muy claro. Para que exista una ciberseguridad el *prius* es el control del código fuente, sin código fuente no puede existir ciberseguridad, es absolutamente imposible. Si no tenemos el código fuente de lo que nosotros estamos manejando no puede existir ciberseguridad. Así es, esa es la cuestión. Tiene usted razón, señor Salvador, porque confundí la Ley de la Ciencia con la Ley de las Universidades. Perdóneme. Me refería a la Ley de las Universidades no a la Ley de la Ciencia.

Con respecto a qué tipo de *software* es aquel que tiene que tener, yo no he hablado del *software* de las personas; las personas pueden hacer con su vida lo que ellas quieran. Cuando estamos en funciones de tipo estatal entiendo que, dado que actualmente lo que estamos haciendo es normando, generando normas jurídicas mediante un *software* —Romanones, el Romanones digital: haga usted la ley y el reglamento y déjeme la aplicación informática— entiendo que estamos en dos supuestos: o en la aplicación informática con la que estamos realizando un trabajo de gestión —donde están derecho fundamentales u ordinarios de los ciudadanos— o en un *software* de control. En esos dos supuestos se tienen que producir los mismos requisitos para esa elaboración de *software* que los que tienen las normas jurídicas. Y los requisitos de las normas jurídicas son el principio de las fuentes del derecho, que son los que ya enumeré. No me extenderé, porque quisiera acabar con una cuestión, bajar a la praxis.

Si bajamos a la praxis, el Programa Afirma, vemos cómo se está haciendo el Programa Afirma por parte de las administraciones públicas. Así es como hay que hacer todo ese *software* de gestión y todo ese *software* de administración, poniendo el código fuente en la red y desde ahí que los ciudadanos podamos hacer nuestras aportaciones. El Programa Afirma, por tanto, nos está dando el modelo de cómo hay que bajar a la praxis, de cómo se está haciendo, de cómo podemos acceder a ese código y de cómo, cuando ese código no nos funciona en ese ordenador, se lo podemos decir a la Administración publica, podemos ejercer el artículo 23.1 de la Constitución española que es el de participación por parte de la ciudadanía. Creo que esto, además, enriquece mucho y tiene unas funciones educativas para la ciudadanía española. Es a lo que me refería con respecto a esa cuestión.

Con esto entiendo finalizada mi aportación. Me pongo a su disposición y mandaré los textos correspondientes que pueda tener, tanto míos como de diversos autores que puedan ilustrar este tipo de pensamiento para la Comisión.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor De la Cueva por su comparecencia y su trigésimo aniversario. Llevamos unos días celebrando trigésimos aniversarios de varias personas e instituciones. Con esto cerramos esta comparecencia. **(Pausa).**

— DEL SEÑOR CAVANILLAS DE SAN SEGUNDO (CHIEF BIG DATA & SECURITY OFFICER, RESPONSABLE DE CIBERSEGURIDAD DE LA EMPRESA ATOS), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/001553 y número de expediente del Senado 715/000617).

El señor **PRESIDENTE:** Señorías, damos la bienvenida y agradezco su presencia a don José María Cavanillas de San Segundo, chief big data and security officer, cuya comparecencia ha sido solicitada por el Grupo Mixto, en concreto por el señor Yanguas.

Doy la palabra al compareciente.

cve: DSCG-12-CM-126

El señor **CAVANILLAS DE SAN SEGUNDO** (chief big data & security officer, responsable de ciberseguridad de la empresa Atos): Muchas gracias.

Estimados señores, en primer lugar, me gustaría agradecerles la oportunidad de dirigirme a este foro que, de entre los varios existentes en el Congreso de los Diputados, está abordando un tema de rabiosa actualidad. La empresa Atos, que aquí represento, tiene en España más de 6000 trabajadores y es una empresa europea de servicios digitales, con sede central en Bezons, en el área de Paris. Nuestro chief technology officer, Philippe Vannier, es el presidente de la ECSO, la European Cyber Security Organisation, Organización europea de ciberseguridad. Llevamos más de veinte años desarrollando tareas de investigación, desarrollo y aplicación de tecnologías de seguridad en los sistemas de información, muchas de las cuales se han desarrollado en España. **(El señor vicepresidente, Jiménez Tortosa, ocupa la Presidencia).** De hecho, mi rol en la empresa desde el año 1996 hasta 2015 era el de director de investigación e innovación, antes de acceder al comité ejecutivo. En esta ponencia de ciberseguridad se ha abordado la práctica totalidad de los grandes temas de la ciberseguridad. Se ha hablado de la defensa nacional; de las *fake news*; de la Directiva NIS —por fin traspuesta a la legislación con el Real Decreto-ley 12/2018, de 7 de septiembre, sobre seguridad en las redes y sistemas de información y convalidado por el Congreso de los Diputados el 20 de septiembre—; también se ha hablado de fragmentación de las competencias sobre ciberseguridad; de las infraestructuras críticas y de los riesgos para los internautas. He echado de menos —y ese va a ser el foco de mi comparecencia— un enfoque no tanto sobre las instituciones, sino sobre las personas y también sobre el futuro a medio y largo plazo, que es el esquema temporal que un profesional de la investigación y el desarrollo debe tener en mente.

Comienzo por las personas. Hablaré de las personas que están detrás de los problemas de ciberseguridad, tanto en el lado de los atacantes como en el de los defensores, del impacto social que estos problemas tienen y plantearé a la Comisión cuatro acciones concretas a emprender. Este planteamiento es mío personal, es muy disruptivo pero he llegado a él tras muchos años de trabajo en la materia, por lo que les ruego que lo consideren. Si no lo consideran directamente, al menos sí me gustaría que lo recibieran como elemento para la reflexión.

En primer lugar, igual que en comparecencias anteriores se ha hablado del mundo del cine, querría plantearles una escena de película, escena que luego emplearé en mi argumentación. Se trata de un ataque extraterrestre a la Tierra. En esta escena, con los telescopios de muchos países se ha observado que, paulatinamente, se acerca a la Tierra un enjambre de naves extraterrestres. A medida que van pasando los días se les ve acercándose y se va distinguiendo su gran número y que parece que muchas portan armas. La pregunta es, ¿cómo debería reaccionar la Tierra? En la realidad, la Tierra tendría un problema muy serio para enfrentar este ataque, porque en el planeta Tierra hay más de doscientos países, no especialmente bien avenidos, algunos de ellos no se hablan con otros, y el ejército unido de los extraterrestres se encontraría con una yuxtaposición de países, de tribus humanas armadas que no saben unirse, se coordinan mal, tarde o nunca, y nuestra desunión terminaría siendo la principal causa de nuestra derrota. España es uno de esos doscientos países y, aunque la veamos un gran país —que lo es—, es realmente muy pequeña ante un ataque extraterrestre. Solo siendo conscientes de nuestra pequeñez y desde nuestra sabia humildad, siendo capaces de integrarnos en una estructura mayor, potencialmente planetaria, podríamos tener posibilidades de éxito. Sigamos con la película. En paralelo a que todos los países se ponen de acuerdo en intentar coordinarse, los extraterrestres ya están bombardeando la Tierra. Todavía no han desembarcado pero una nave ha bombardeado con láser una ciudad española y un taller de coches ha quedado destrozado. El hombre del taller piensa: Me he quedado sin taller. El seguro no me cubre ataques extraterrestres y no sé si llamar al Ministerio del Interior, al de Industria, al de Defensa o a la consejería de asuntos alienígenas de mi comunidad autónoma. Y están todos muy liados porque los extraterrestres están bombardeando por todas partes y están pensando en los grandes puentes, en los aeropuertos, en los pantanos pero nadie piensa en mi taller. Y el caso es que hay muchas actas de reuniones de coordinación, hay mucho debate en la tele, puede haber hasta una ponencia en el Congreso de los Diputados sobre qué hacer con los extraterrestres. Mientras tanto, yo me he quedado sin taller.

Aterricemos este caso. Ahora pensemos en el ciberespacio. De algún modo, los ataques en el ciberespacio, que pasan en cualquier momento con efectos inmediatos y con unas tecnologías cuya complejidad van más allá de lo habitual en la mayor parte de los negocios, son parecidos a un ataque extraterrestre. Los humanos detrás de los ataques de ciberseguridad proceden todos de este planeta y todos los implicados son terrícolas, tanto los que impulsan el ataque como el que los recibe, pero los

cve: DSCG-12-CM-126

atacantes no están ligados a un territorio. Un típico ataque de ciberseguridad puede resultar de la acción combinada de una persona en Rusia, una en Túnez, una en Colombia, tres en Canadá, una en Barcelona y otra en La Coruña. Los *hackers*, que al final solo son personas —pueden tener o no ligazón entre ellos—, podrían perfectamente haberse conocido apenas unos días antes del ataque, pero sí tienen en común la voluntad de hacer daño, movida por algunas motivaciones que luego segmentaré.

El ciberespacio no tiene territorio. De algún modo, unifica a los actores con una linealidad mundial y la segmentación de personas y actividades, lo que podría considerarse los países o regiones en Internet, depende de los puntos en común que estas personas tengan, independientemente de su ubicación y también de los pocos escrúpulos que puedan tener, y créanme que en 7000 millones de seres humanos hay margen para muchos segmentos de intereses y de escrúpulos. Así que, no sabiendo de dónde vienen, ni qué quieren, ni cuándo van a atacar, ni cómo y al hacerlo lo hacen en varios sitios a la vez y con tecnologías novedosas para los terrícolas, el ejemplo extraterrestre tiene sentido.

Si analizamos las motivaciones de los atacantes, puedo segmentar nuestros enemigos en el ciberespacio entre grupos. En primer lugar, está el atacante motivado por una razón política, habitualmente vinculada a la seguridad nacional. Un ejemplo claro es el ISIS, el Estado Islámico de Irak y el Levante, pero también incluyo en este segmento agrupaciones de motivación política, comúnmente llamadas hacktivistas, como Anonymous u otras. Un atacante de este grupo utiliza Internet como campo de batalla para conseguir adeptos, recabar datos geográficos o financieros de personas, empresas o instituciones para sus ataques físicos o cibernéticos y potencialmente atacar aquellos objetivos que se fije, empleando total o parcialmente la red mediante *software* malicioso, ataques tipo DDoS, o quizá ataques dirigidos a infraestructuras críticas, bien informáticas o bien físicas, empleando Internet de las cosas. Es importante la extensión física del ataque cibernético. Yo, atacante, consigo por la red información para actos terroristas que luego ordeno a través de la red y que mis adeptos ejecutan causando muertos, heridos y daños materiales cuantiosos en el mundo físico.

En segundo lugar, está el atacante vinculado a un objetivo económico. Este puede ser el tráfico de armas, de imágenes pornográficas no consentidas o prohibidas, como la pedofilia, u otros productos al margen de la ley y también aquellos que proceden a emplear *software* malicioso para bloquear una base de datos o un servicio y pedir rescate por él, conocido como *ransomware*. También hay que incluir en este grupo el ciberataque silencioso, aquel que simplemente recoge información sin dañar en ese momento un producto o servicio, información que luego se puede utilizar para conseguir un objetivo económico en otros entornos. Ejemplos de ciberataques silenciosos son: la obtención de información industrial secreta para la competencia; la información financiera sensible para su utilización en los mercados de valores; la obtención de datos médicos privados de las personas o la afiliación o pertenencia a colectivos sensibles que luego pueden ser usados en contra de la persona.

En tercer lugar, está el atacante vandálico, el que no tiene objetivo político ni económico, sino simplemente la malsana satisfacción de haber sido capaz de hacer daño. Si bien el vandalismo existe en el mundo físico desde hace siglos y afortunadamente en España es poco frecuente, en el caso del ciberespacio este tipo de ataque es sorprendentemente muy frecuente y está ligado a problemas de personalidad de los atacantes y supuestamente protegido por el anonimato que se puede conseguir en Internet en ciertas condiciones. También influye la posibilidad de hacerlo desde una ubicación física propia de confianza, desde un domicilio, y la posibilidad de alcanzar un objetivo lejano físicamente, potencialmente internacional y a personas o entidades de renombre.

Ahora segmentaré los atacantes por perfil social. Los perfiles habituales son los siguientes: el primero, el solitario; una persona que en el mundo físico no crea problemas ni despierta sospechas, pero en la privacidad de su domicilio se dedica a actividades ilegales, solo o en connivencia con otros individuos a los que conoce por Internet, formando una red de ciberdelincuencia *ad hoc* y que están ubicados en territorios o franjas socioeconómicas muy dispares. De nuevo, esas regiones de Internet de las que no hay mapas. El segundo, el delincuente profesional que, sin ser un solitario, actúa en una red criminal con objetivos económico, sexual o político ya existente en el mundo físico y emplea el ciberespacio como un territorio más para la comisión de sus delitos. El tercero, el *insider*, una persona que se encuentra dentro de una organización cuya motivación ha pasado a ser negativa por una o varias razones, que decide actuar contra el ministerio, empresa u organización dentro de la cual está. En general, dado que se encuentra dentro, accede a una información mucho más sensible y más veraz que los otros dos y su capacidad de hacer daño es mucho mayor.

cve: DSCG-12-CM-126

Todos estos ataques impactan en nuestra sociedad en cuatro ámbitos. El primer ámbito es la seguridad de las infraestructuras críticas, de la que ya se ha hablado largamente en esta Comisión. Adicionalmente, este ámbito está explícitamente mencionado en el artículo 2 del Real Decreto-ley 12/2018, de 7 de septiembre, ya mencionado. Aquí se incluyen también las grandes empresas que dan servicios digitales. El segundo ámbito son las grandes empresas e instituciones que, sin ser infraestructuras críticas, su actividad incorrecta o inactividad producida por un ataque tiene repercusión mediática. Son susceptibles de ataque o por *insiders* o por organizaciones delictivas o por solitarios que las identifican por su visibilidad de tamaño. Es frecuente que las grandes organizaciones se doten de medios para defenderse de todo ataque de ciberseguridad.

Un buen ejemplo son los Juegos Olímpicos. En los últimos Juegos Olímpicos de Verano, Río 2016, Atos, mi empresa, tuvo la responsabilidad de la ciberseguridad y estoy orgulloso de decir que en catorce días de juegos hubo más de 5000 millones de incidentes de ciberseguridad, con cero impacto en la operativa de los juegos. Este éxito, como todo otro éxito de blindaje ante los ciberriesgos, se basa en el trabajo de muchas personas y, obviamente, en un desembolso importante de recursos que solo las grandes empresas pueden abordar.

El tercer ámbito son las pymes y autónomos en el ejercicio de su actividad profesional. Las pymes se encuentran en una situación de desprotección enorme, debido, sobre todo, a la necesidad de inversión para su protección. Una gran empresa se puede pasar, por ejemplo, 1 millón de euros en proteger miles de puestos de trabajo contra ataques *endpoint* y a sus servidores contra ataques de denegación de seguridad de servicio, pero las pymes no pueden acceder a esos desembolsos para protegerse de los mismos peligros. Volviendo al caso anterior, si un taller de coches recibe un ciberataque y se inutiliza su sistema informático, el efecto es similar a que le haya caído un rayo láser de una nave extraterrestre: su negocio se ha frenado o destruido y el daño en su pequeña economía es enorme y potencialmente irreversible. Es verdad que el Incibe tiene recomendaciones de protección enfocadas a las pymes que ayudan a evitar muchos peligros, pero que no blindan a estas empresas contra los ciberataques, aunque sí les ayudan y son muy bienvenidos, pero puedo afirmar que muchas de ellas ni siquiera conocen que hay un teléfono de asistencia de la Oficina de Seguridad del Internauta; incluso algunas de ellas ni siquiera se verían reflejadas en la palabreja internauta, simplemente tienen un taller y el ordenador ha fallado. Y es importante resaltar que en este ámbito de las pymes, sin ser formalmente una infraestructura crítica, es desde luego un ámbito crítico para el funcionamiento de la economía española. En 2018 el 99,88 % de las empresas españolas eran pymes y generaban el 66 % de los empleos de la nación. De los 16 millones de asalariados en 2018, 10,5 millones trabajaban en pymes. Adicionalmente, por si estos datos pudieran todavía no llegar a concluir la criticidad de las pymes en el funcionamiento del Estado, lo cierto es que hay muchas grandes empresas que para funcionar necesitan una red de pymes dándoles servicio, y pongo por ejemplo una empresa de automoción que requiere proveedores locales, generalmente pequeños, de elementos y servicios. Si un ciberataque inutiliza esa red de pymes, da igual lo bien protegida que esté la empresa grande, el proceso de producción de automóviles se ha parado. Y no piensen solo en automóviles, piensen en telefonía, energía, leche, magdalenas, papillas para niños, medicinas, hospitales, etcétera. Muchos servicios estatales están considerados como infraestructuras críticas y dependen a la vez de muchas pymes, por lo que la exposición que las pymes tienen ante los ataques en el ciberespacio pone en riesgo también a los dos primeros ámbitos.

Hagamos una pequeña reflexión de nuevo sobre la pyme. Este taller que ha recibido un ciberataque —y les pongo un ejemplo concreto—, en el que un *ransomware* ha secuestrado los datos de un ordenador central, no es solo un ejemplo, fue un caso real muy ilustrativo. Al hablar con la persona del taller, me explicó que se habían perdido todos los datos de clientes, de automóviles reparados, de alarmas e incluso de los coches que estaban ahora mismo en tránsito; no tenían información de qué necesitaban. Claro, siempre pueden preguntárselo a los dueños de los coches. ¡Ah, no! ¡Que los teléfonos de los dueños estaban en la base de datos! No podemos llamarles. El dueño del taller nos explicó que se había perdido todo —enlaces con proveedores de piezas usuales e inusuales, acceso a sistemas automatizados de provisión, todo— y nos pidió que, si podíamos, desencriptáramos ese disco duro que había encriptado el *ransomware*. Le recomendamos que aplicara la copia de *backup* y nos explicó que ya lo había intentado pero que el sistema de *backup* también había quedado infectado. Le explicamos que un proyecto de desencriptación de un disco duro dependía de la complejidad de lo encriptado y, si era posible, como mínimo se necesitarían varios consultores, varios meses y no bajaba de los 100 000 euros. Nos respondió literalmente: ¡Sí, hombre! ¡Si yo tuviera 100 000 euros, iba a estar yo aquí arreglando coches! ¡Vamos,

cve: DSCG-12-CM-126

digo yo que las grandes empresas estarán todas muy protegidas, pero mis datos…! Nadie viene aquí a recuperarme mis datos. ¿Qué hago —me dijo—, me meto en otro ordenador y les pago el rescate, los 300 *bitcoins* esos que me piden? Yo le recomendé no hacerlo: es fácil que sí cobren el dinero y tú nunca puedas recuperar tus datos. Dijo: Ya, pero para mí esto es el fin. Allí tenía las nóminas, el sistema, las deudas pendientes, los dineros que me deben. Es el fin. Un rayo láser había caído en su taller y ya no había taller. Haya o no haya decreto-ley, antes y después del decreto-ley —que tan bienvenido es, que tanto tiempo ha costado a hacer a sus señorías y que tantas cosas soluciona en otros ámbitos—, lo cierto es que el foco es la Directiva NIS y no otros aspectos, y la situación para el taller es la misma: nadie le soluciona nada.

El último ámbito son los ciudadanos del Estado español y, desde un punto de vista general. Me refiero a un ciudadano usando su ordenador para pagar los impuestos o ayudar a sus hijos en el colegio, o a aquellos colectivos especialmente sensibles, como los menores, la tercera edad y los discapacitados. El Incibe también tiene recomendaciones concretas para estos colectivos y de nuevo son muy bienvenidas, pero no blindan al ciudadano contra ataques. De especial importancia son los daños que pueden hacer a los menores, y la pedofilia es un muy triste ejemplo de ello. En cuanto a la tercera edad, los ancianos están muy expuestos a muchos incidentes; por ejemplo, a timos por Internet, como correos bancarios falsos como el *phishing*, que potencialmente les pueden crear un problema financiero severo. Lo peor de todo es el riesgo de las instalaciones domóticas para personas con necesidades especiales: los ciberataques contra instalaciones que facilitan la vida a personas con discapacidad pueden simplemente acabar con su vida.

Tras haber hablado de los atacantes y del impacto de los ataques, permítanme hablar un momento de los defensores, las personas detrás de la defensa. Una empresa que se dedica a la ciberseguridad debe contar en su nómina con personas con los conocimientos técnicos que el ciberespacio requiere. Son muchos perfiles diferentes, que van desde simples operadores de centros operativos de seguridad, pasando por expertos en herramientas SIEM o evaluación de riesgos, hasta *hackers* profesionales con capacidad de atacar y, por tanto, evitar un ataque, que reciben el nombre de tigres. Un equipo de tigres recibe el nombre inglés de *tiger team*, un grupo de *hackers* que actúa contra los *hackers*. Pero tener tigres en casa no siempre es bueno, a veces te muerden. Si tú contratas a un experto en la Internet profunda, por alguna razón será un experto en la Internet profunda, y no siempre la razón es la que explica en el currículum; quizá la aprendió en un curso de formación especializada, quizá la ha aprendido en un grupo delictivo al que pertenece o al que puede terminar perteneciendo, quizá ambas cosas. Lo más complicado para un gestor de equipos de tigres es asegurar que esas personas con tanta capacidad para frenar ataques no se han metido en tu equipo o en tu ministerio con el objetivo de terminar atacando desde allí o, aunque no se hayan metido con ese objetivo, puedan terminar teniendo ese objetivo.

En este sentido, el problema no es un problema tecnológico, es un problema humano, de nuevo relacionado con las personas. Es preciso asegurar en los profesionales de la defensa ante ciberataques que su intención está alineada con los intereses del Estado o de la empresa y que no van a comportarse de pronto como solitarios o como *insiders*, y para ello es preciso darles mucho más que un empleo; hay que darles una formación reglada, una motivación, una carrera a largo plazo, un objetivo vital de defender el bien ante el crimen. Lo mismo que cuando le das una pistola a un policía y esa pistola que le das puede matar, pero antes de dársela el policía pasa por la academia y todo el esfuerzo que él ha puesto para llegar a merecer esa pistola nos garantiza que no traicionará los objetivos de su institución. Igualmente, poner un tigre a defender tu empresa o tu país en Internet conlleva de forma inherente un riesgo. Un buen tigre puede ser muy útil para nuestra nación, si él quiere. Pero contratar un tigre no puede ser simplemente leer un currículum, contratarle y ponerle a pegar tiros en la cibertrinchera; debe haber mucho más.

Pero dejemos de hablar de problemas y hablemos de soluciones. Hay una solución para las pymes. Y frente al debate que hay sobre la fragmentación o no de las competencias en ciberseguridad, aquí me gustaría reivindicar la capacidad de acción local. Es muy importante la cercanía con la pyme, y las comunidades autónomas son especialmente indicadas para esta solución. La solución debe ser la misma que se emplea con las grandes empresas: acometer grandes inversiones de protección de servidores y de puestos de trabajo, pero no de la gran empresa, sino del conjunto de pymes. Una sola inversión, muchas pymes beneficiadas, una pequeña contribución de cada una. Para poder acometer estas inversiones es preciso la intervención de las asociaciones de pymes, territoriales o sectoriales, y una muy enfocada acción de las consejerías de Industria de las comunidades autónomas, apoyando logística y financieramente —voy a repetir la palabra, financieramente— a las pymes del territorio para dotarlas con

cve: DSCG-12-CM-126

las mismas herramientas y servicios que piden las grandes empresas: herramientas tipo SIEM, centros operativos de servicios SOC de uso colectivo, herramientas *endpoint* para producción de puestos de trabajo, protección ante denegación de servicio, control de acceso a las redes y subredes y vigilancia constante y prescriptiva de amenazas puntuales o persistentes.

Adquirir esas herramientas y financiar esos servicios empleados de modo colectivo requiere la unión de muchos y, de nuevo, la intervención directa de las consejerías de Industria para proteger su tejido industrial. Ese gasto es una inversión con un retorno importante: si no se invierte, la cantidad de dinero que la comunidad autónoma va a perder por pérdidas ligadas a cibercrimen es enorme; si se invierte, se asegura el funcionamiento correcto del tejido industrial de pymes, que es, en muchos territorios, la infraestructura crítica por excelencia de la economía local. No debemos aspirar a que el taller conozca o no el teléfono del internauta, es preciso que la asociación de talleres de su ciudad acuerde con la comunidad autónoma la utilización de un centro operativo de seguridad SOC y de unas herramientas de calidad y que, mediante copago, un taller pueda permitirse una inversión y tener una protección de calidad. Ya sé que la palabra copago está muy denostada, pero no tengo otra que defina qué parte del coste y servicio de la herramienta lo haga la pyme —una parte del coste razonable— y que la otra parte la acometa la comunidad autónoma. Soy reacio a los servicios gratis —esto requeriría una larga explicación— y también sé que una pyme no puede permitirse el coste completo. La Consejería de Industria debe actuar como consejería de asuntos alienígenas y proteger a sus talleres de los ataques láser.

Asimismo, los colectivos de ciudadanos, especialmente los sensibles, requieren una acción paralela por parte de las consejerías de Asuntos Sociales, especialmente la creación de puntos de respuesta ciudadana, teléfonos de atención a la persona para evaluar si ha tenido un problema de ciberseguridad y cómo salir de él. Pero no solo el teléfono del Incibe —que, insisto, es muy bienvenido—, tu comunidad, tu ayuntamiento, tu asociación de discapacitados debe habilitar en todas las líneas de capilaridad posibles vías de comunicación para la población. Para ello, la contribución logística y financiera de las consejerías de Asuntos Sociales es fundamental. De nuevo, ¿he dicho financiera? Sí, he dicho financiera.

Hago una pausa en mi disertación para trazar una línea más disruptiva aún en el discurso. Hace ciento nueve años se menciona por primera vez a la aviación militar en la Real Orden del 2 de abril de 1910. En aquel entonces existía la Armada española y el Ejército de Tierra, y nada más. La asignación de aviones al ejército se decidió ubicar en el cuerpo de ingenieros del Ejército de Tierra; nadie pensó entonces en otra opción. Tendrían que pasar más de veinte años para que el combate en un terreno nuevo, el aire, cuyas técnicas de combate, tecnologías implicadas y formación necesaria, que eran tan distintas del mar y de la tierra, pudiera merecer la creación de un tercer ejército, el Ejército del Aire. Pero estamos en 2019. A día de hoy, afortunadamente, nadie está atacando a España por el aire, nadie por el mar, nadie por la tierra, y sí hay, desgraciadamente, muchísimos ataques en el ciberespacio que afectan a los ámbitos de Defensa e Interior; un nuevo territorio, distinto de los otros tres, cuyas técnicas de combate son distintas, cuyas tecnologías implicadas son muy diferentes y cuya información es tan compleja. A mi entender, en este momento de la historia se requiere una decisión valiente, con visión, que es la creación de un cuarto ejército, el ejército de la red. Un nuevo ejército donde los profesionales puedan hacer su carrera vital, donde los tigres puedan formarse para luchar por España y para España, y que tras treinta o cuarenta años de servicio, puedan acabar como los grandes generales del ejército. Un compromiso doble: ellos se comprometen con España y España con ellos, al igual que los otros tres ejércitos. Un ejército que actúe en los ámbitos de Defensa y de Interior, pues los ciberataques cubren ambos ámbitos y ya tenemos en España un cuerpo en el ámbito de Interior con reglamentación militar, que es la Guardia Civil.

Con esto no quiero menospreciar a todos los organismos que a día de hoy trabajan en la defensa de los ciudadanos y de las empresas, sino al revés, ponerlos en valor: al Consejo Nacional de Ciberseguridad, que define y ejecuta el Plan Nacional de Ciberseguridad; en el ámbito de Defensa, el Mando Conjunto de Ciberdefensa, que concentra y unifica muy acertadamente las actividades del Ministerio de Defensa en este entorno, que para mí es un muy acertado primer paso; en el ámbito de Interior, las Fuerzas y Cuerpos de Seguridad del Estado, que cuentan con varias unidades para combatir los ciberataques, como el Grupo de Delitos Telemáticos de la Guardia Civil, la Brigada de Investigación Tecnológica de la Policía Nacional, la Unitat Central de Delictes Informàtics de los Mossos d'Esquadra, la Sección Central de Delitos de Tecnologías de la Información de la Ertzaintza y el Grupo Especializado en Delitos Informáticos de la Policía Foral de Navarra. Adicionalmente, están CNPIC para protección de las infraestructuras críticas, el Centro Criptológico Nacional, el Departamento de Seguridad Nacional en Presidencia del Gobierno, el Incibe en el Ministerio de Industria, y a escala internacional, debemos conectar nuestra actividad con

cve: DSCG-12-CM-126

la ONU, la OSCE, la OTAN y la Unión Europea y su Estrategia Europea de Ciberseguridad. Es importante remarcar que el artículo 13 del real decreto-ley establece que hay un punto de contacto único, el Departamento de Seguridad Nacional, para la cooperación transfronteriza.

Todas estas líneas ya están trazadas, todos estos cuerpos actúan coordinados y alineados en esta materia, pero yo propongo ir un paso más allá. Al igual que tenemos el Ejército del Aire, EA, el Ejército de Tierra, ET, y la Armada Española, AE, deberíamos tener el ejército de la red, el ER; ejército que a su vez debe integrarse en las estructuras internacionales correspondientes. España es muy pequeña para este problema. Solo podríamos ganar una batalla en el ciberespacio si actuamos conjuntamente con las naciones vecinas europeas y con todas aquellas que estén de acuerdo en la defensa de la economía y del modo de vida alineado con el español. Para la sociedad civil haría falta algo más. La humanidad lleva miles de años haciéndose daño en el mundo físico y las espadas matan igual a Julio César hace dos mil años que nos pueden matar hoy. Hemos aprendido los riesgos y medidas de protección que los peligros físicos tienen. Nadie dejaría a un niño solo con un cuchillo; sin embargo, sí dejamos un niño solo con un móvil, y también tiene peligro. El ciberriesgo es tan reciente que la mayor parte de la gente todavía no ha aprendido a gestionarlo. Hace solo treinta y un años del primer delito informático —el gusano de Morris, en 1988— y en treinta años la cantidad de maneras de hacer daño en la red solo ha crecido y de manera exponencial: mucho daño, muchas maneras y cada año nuevas. En 2010, nadie sabía lo que era un DDoS; hoy, los DDoS han creado una enorme cantidad de pérdidas materiales. ¿Qué nuevas maneras aparecerán de aquí a 2020, a 2025 y a 2030? Es preciso un mecanismo de aprendizaje rápido de los peligros nuevos y la capacidad de formar rápidamente a profesionales para enfrentar estos nuevos retos, no solo los que conocemos hoy, sino todos los peligros que están por venir.

Creo que es precisa la creación de grandes centros de formación de alto rendimiento de profesionales cibernéticos, centros conectados con las fuentes de información de riesgos cibernéticos en tiempo real, que formen rápidamente sobre los nuevos peligros a los profesionales; centros que deben ser más una academia de policía o militar que una facultad. No solo es aprender la tecnología, es crear profesionales alineados en motivación. Los profesionales que salgan de esas academias podrían continuar su carrera en el ejército de la red o en la empresa privada y de ese modo la empresa tiene la garantía de que ese ciberprofesional ha comprometido su vida en la defensa del bien en el mundo cibernético. Es importante mencionar que esto es exactamente lo que se ha propuesto el presidente Xi Jinping. La República Popular China se plantea crear entre 2017 y 2027 seis academias de formación cibernética de talla mundial y la creación de un ejército de Internet en la República Popular China.

Para terminar, resumo las cuatro propuestas concretas que traigo hoy. Uno, acción por parte del Ministerio de Asuntos Sociales y consejerías de Asuntos Sociales de las comunidades autónomas: una acción específica destinada a proporcionar información, formación, herramientas y servicios de ciberseguridad a colectivos desfavorecidos, mayores, menores y discapacitados, y una línea básica al ciudadano de a pie. Dos, acción por parte del Ministerio de Economía y consejerías de Economía de las comunidades autónomas: una acción concreta para dar servicio de ciberseguridad a las pymes y autónomos mediante acuerdos de protección con asociaciones regionales y sectoriales. Tres, creación del ejército de la red con ámbito de su aplicación en el campo de Interior y Defensa, y su posterior integración en las entidades supranacionales de defensa cibernética. Cuatro, creación de las grandes academias de profesionales de ciberseguridad, profesionales motivados y preparados para la defensa de nuestra nación, de nuestros ciudadanos y empresas, y la protección de nuestro modo de vida.

Esta es mi reflexión y estas son mis propuestas. Muchas gracias por su atención.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, don José María Cavanillas por la ilustrada exposición con la realidad.

A continuación, tienen la palabra los representantes de los grupos políticos y después tendrá ocasión de contestar. En primer lugar, por el Grupo Mixto tiene la palabra el señor Yanguas.

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

En primer lugar, y antes de hablar de la ponencia propiamente dicha, como no intervengo en todas las comisiones, me gustaría agradecer una vez más al presidente de la Comisión, a la Mesa y al letrado el trabajo que se está haciendo durante estos meses en esta ponencia, porque al final creo que tendremos unas conclusiones importantes y, sobre todo, trabajadas por parte de muchos expertos de cara al futuro sobre lo ciber y sobre el posicionamiento de nuestro país en este campo. También me gustaría agradecer que en el día de hoy comparezca un experto como usted, señor Cavanillas, que, como ha dicho el

cve: DSCG-12-CM-126

presidente, ha sido propuesto por el Grupo Mixto, que ha tenido a bien hacer un hueco y tenerle hoy aquí, en el Congreso de los Diputados.

En cuanto a la comparecencia, quiero darle la enhorabuena, no puedo hacer otra cosa tras escucharle, por esa clara exposición práctica —al menos yo lo he visto así—, ligada a la tierra, que ha venido a aclarar algunas cuestiones y a tratar otras cuestiones nuevas que no se habían tratado aquí —por lo menos a mí no me consta que haya sido así— en materia de seguridad. Desde el inicio, ha logrado captar nuestra atención —por lo menos la mía— con la historia de los extraterrestres. Ha empezado usted en el espacio pero pronto ha aterrizado en la tierra, logrando captar la atención por lo menos de este portavoz. En concreto, que usted hoy haya focalizado la exposición sobre las personas y sobre las pymes, creo que es algo importante y usted ha dado unos datos que así lo reflejan y que caen por su peso. Desde luego, coincido con usted en las conclusiones que nos ha planteado y nos ha mandado trabajo que hacer. Lo cierto es que no pensaba hacerle ninguna pregunta, pero ha citado usted a la Comunidad Foral de Navarra, en concreto, a la Policía foral de Navarra. Como usted sabe, como todos ustedes saben, soy de un partido, Unión del Pueblo Navarro, que se presenta solo por una comunidad, por la Comunidad Foral de Navarra, y me gustaría que ampliase, si pudiera, la información sobre cómo implantaría o como se podría implantar ese centro que ha citado, ese SOC, para las muchas pymes que están instaladas en toda España. Yo querría centrarme en la Comunidad Foral de Navarra y saber si usted podría ampliarme esa medida con el fin de ver, desde el punto de vista de una persona que no está en el mundo de la ciberseguridad, cómo se podría implantar o cómo podemos trabajar los legisladores o también el propio Parlamento y el Gobierno de Navarra, y que eso fuera una realidad en nuestra Comunidad Foral de Navarra.

Concluyo dándole las gracias de nuevo por su trabajo y por abrir hoy aquí este debate sobre las pymes, sobre las personas que, a mi modo de ver, hacen todavía más importante y más visible la ponencia en la que hace unos meses nos embarcamos en esta Comisión Mixta de Seguridad Nacional.

Muchas gracias, señor presidente.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señor Yanguas.

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

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

En primer lugar, deseo felicitar al compareciente. Decía yo al compareciente anterior que era muy complicado a estas alturas de la Comisión, con la cantidad de comparecientes que han concurrido —que han sido muchos y de ámbitos muy diversos—, que hubiera personas que aportaran cosas diferentes a lo que se había aportado hasta ahora. Al igual que se lo dije al compareciente anterior le digo a usted que está trayendo a esta Comisión algo —quizá lo más importante de todo lo que estamos hablando— que no había sido aportado anteriormente: el tema de las personas. Incluso yo a todos los comparecientes, en el momento de formular las preguntas, les dejaba caer la importancia del usuario final, de las personas, algo que usted también ha extendido a la economía, a las pymes y a la importancia que eso tiene también para el empleo. Por tanto le felicito por ello.

Me ha gustado mucho la plasmación en propuestas concretas y a la vez pragmáticas sobre dónde se tienen que desarrollar y se pueden desarrollar, viendo todo el esquema que está funcionando. No se trata tanto de tener principios filosofales como de decir: la Consejería de Asuntos Sociales puede aportar esto, la Consejería de Industria puede aportar esto otro, y el Ejército se tiene que configurar también entendiendo que estamos ante una nueva realidad, lo cual comparto plenamente. Me ha gustado mucho lo que ha dicho de los tigres; es verdad, se necesita precisamente a personas que han estado en ese submundo porque son las que han profundizado en él, lo conocen, y porque no hay gente formada para ello. Otra cosa distinta es formar a los buenos en penetrar en esos mundos, en aprender de ellos y saber cómo tienen que actuar y defendernos. Comparto con usted también que es un riesgo contar con personas que en un momento determinado estuvieron en un lado y puedan estar otra vez en el mismo o puedan ser susceptibles de ser captadas por mafias. Igual que una oferta les ha podido captar para trabajar en el lado de los buenos o para evitarse problemas con la justicia o cualquier otro, también son susceptibles de una mejor oferta que pueda hacer que cambien de bando. Por ello mi grupo comparte plenamente la creación de esas grandes academias de formación que den respuesta a una nueva realidad, porque en el fondo es lo que hemos reclamado también a todos los comparecientes, es decir, saber qué tipo de perfiles, qué tipo de reformas, qué tipo de educación tiene que haber para garantizar que tengamos respuesta a todo esto. Simplemente le añadiría una pequeña pata a los cuatro elementos que usted ha comentado, que son muy buenos, y es la formación del usuario final para que también contribuya a esa nueva forma de defenderse,

cve: DSCG-12-CM-126

sabiendo utilizar adecuadamente todo y sabiendo cómo no incurrir en los peligros. Igual que todo el mundo sabe dónde están los peligros en el mundo analógico, se debe también saber dónde están los peligros digitales y cómo poder evitarlos.

Muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señor Salvador.

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

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Bienvenido a esta Comisión, señor Cavanillas. Muchas gracias por su exposición. Era imprescindible para este trabajo que en algún momento hiciésemos aterrizar los discursos macro a lo realmente diario e imprescindible, que era la perspectiva ciudadana y de las pymes, que suponen al final el grueso de las interacciones que se puede tener a muchos niveles, y creo que usted lo ha hecho magníficamente bien a lo largo de hoy. Es muy interesante profundizar —y su trayectoria profesional puede aportar también mucho a este respecto— en las relaciones entre la empresa publica y la privada. Hemos debatido muchísimo sobre cómo hay que hacerlo, sobre si lo estamos haciendo bien o mal, sobre si hemos profundizado en lo que deberíamos o no, sobre si las empresas privadas tienen el suficiente conocimiento de lo que los recursos públicos les dan, sobre cuándo pueden conectarse, si la legislación llega a los lugares que debe llegar para que las empresas privadas conozcan sus obligaciones, pero sobre todo sobre cómo se establece ese mecanismo imprescindible de relación entre la empresa pública y la empresa privada. Creo que esta experiencia profesional que usted acumula en el ejercicio de su actividad puede ser muy interesante para marcar determinadas pautas.

Como ha sido tan propositivo a lo largo de su primera intervención me permito la licencia de pedirle que nos lance alguna propuesta concreta también a este respecto. Existe otra relación entre el sector público y privado que hace que tengamos que trabajar juntos, que son no solo las inversiones en I+D+i, sino los programas y los objetivos que deben tener nuestra inversión y nuestros proyectos públicos en I+D+i. Nosotros somos muy críticos a ese respeto y creemos que no se está haciendo el esfuerzo necesario. Consideramos que no hay un proyecto de futuro y que, por lo tanto, no solo no se están sabiendo leer cosas que marquen un sistema rentable, puntero y de futuro, sino que además la actuación no está sirviendo para atraer talento, para formar talento, y para permitir que este talento luego repercuta en nuestro sistema estatal.

Si hay un espacio de protección ciudadana que es imprescindible garantizar cuando hablamos de seguridad de la información y de protección de datos es todo lo dedicado a la atención sanitaria y al espacio sanitario. Lo es porque hay un volumen enorme de datos y de información que se maneja, y esta información siempre es sensible, pero es que además esa información siempre es totalmente privada, y por lo tanto hay que garantizar la privacidad de esa información. Es importante además no solo porque sea un sector público muy conocido por la ciudadanía, sino porque es además un sector público con un uso permanente por parte de la ciudadanía. Hay una experiencia que hila todo lo que acabo de relatar, que fue la experiencia que Atos y el Sergas hicieron en Galicia respecto del laboratorio de seguridad en la información. No solo seguimos con mucha atención eso las gallegas, porque evidentemente se nos iba mucho dinero y seguridad de la información en ello, sino porque la sensación era que se estaba creando un nuevo nivel de gestión en servicios de seguridad tan complejos como era plantear un espacio seguro para la gestión de los datos sanitarios y médicos. Creo que se resolvió satisfactoriamente. La pregunta es si había alguna necesidad específica que tuviera el sector sanitario. He hecho un poco las mismas preguntas a quien ha trabajado con la experiencia privada, como ha sido el caso del anterior compareciente en el sector jurídico, y se lo pregunto a usted ahora. ¿Había alguna necesidad específica que hiciese que ese laboratorio fuese diferente cuando se hablase de gestión médica? Quisiera saber si esa experiencia, que por lo menos en España fue un espacio de colaboración público-privada que no se ha dado muchas veces —por lo menos, no se ha conocido tan en profundidad; puede que sí exista, que yo lo desconozca y que a mí me haya aparecido más cercano en la información, y que haya permitido seguir el hilo del proyecto hasta su término—, tenía alguna de esas necesidades específicas, y si este proyecto se puede extrapolar a algún otro espacio del sector público, y es aplicable ese marco de colaboración público-privada que pocas veces me consta que se haya dado.

Sobre la propia experiencia en sí me gustaría conocer cuáles son los pasos prácticos. Quisiera que nos detallara, de forma muy breve —si es posible resumirlo, porque entiendo que sería complejísimo—,

cve: DSCG-12-CM-126

cuáles fueron los objetivos y cuál fue el hilo seguido al respecto para proteger y garantizar la seguridad de la información en este campo, en el que —y repito, creo que fue muy importante— sigue considerándose ese espacio como un antes y un después en el nivel de gestión de seguridad en espacios complejos como era el de la sanidad.

Nada más. Muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señora Angustia.

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

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

En primer lugar, quiero agradecer al señor Cavanillas, en nombre del Partido Socialista, que esté aquí trabajando con nosotros y que nos traslade, fruto de su experiencia, los conocimientos que ha adquirido porque nos ayuda y nos facilita crear en la ponencia los contenidos y establecer las prioridades, que de eso se trata.

Tengo dos o tres preguntas que quizá amplíen un poco algunos de los aspectos que ha señalado, aunque no tengan relación con mucho de lo que ha planteado, porque precisamente las que tenía yo preparadas tenían que ver con prioridades a la hora de la intervención o la actuación que tenían que tener los poderes públicos, cuáles serían los puntos de mejora o cómo corregir los puntos débiles. En concreto me gustaría que nos dijera, fruto de la experiencia y del largo recorrido que tiene ya, qué opinión tiene sobre la existencia del anonimato en la red, cómo cree que va evolucionando o avanzando la identificación de la máquina de la que provienen los ataques, efectivamente hablando. Hemos hablado en muchas ocasiones de la posibilidad de que existan máquinas zombi que se puedan manejar desde otros centros por otra persona, de forma que los ataques en principio parecen originarse en esas máquinas que están manipuladas, pero me gustaría saber cómo va avanzando la posibilidad de identificar con realidad la máquina original de la que procede el ataque. Aquí tenemos un problema. Yo soy mucho más partidario de la prevención y de la promoción de capacidades —prevenir los ataques, promover las capacidades—, pero hay un problema también a la hora de responder contra los agresores, bien sea por la persecución de un delito o bien sea por la agresión incluso en colaboración con un Estado a otro Estado. En muchísimas ocasiones eso se queda un poco en el aire, porque todavía parece ser, entre comillas, que no está muy avanzada, por lo que sabemos, la identificación del origen concreto de esos ataques. Entonces, cuando el interés de un Estado es atacar a otro para originarle una debilidad y obtener una supremacía o hegemonía a nivel mundial o en una zona o región del planeta, los Estados tienen que tener capacidades también de respuesta, no solo de prevenir los ataques, sino de poder defenderse en el sentido de contraatacar.

La otra cuestión tiene que ver con el aspecto organizativo, al que creo que ha dado también bastante importancia. A ver si nos lo podría ampliar un poco más en el sentido de evaluar si cree que con la complejidad que puedan tener las estructuras que hoy día manejamos, tanto a nivel europeo como a nivel estatal fundamentalmente, eso ayuda, ya que se necesita una gran capacidad de funcionalidad, de dirección y de toma de decisiones a la hora de obtener respuesta rápida. Si la organización que tenemos ahora mismo, más allá de que pueda ser más o menos transversal, facilita ese proceso de toma de decisiones y una respuesta rápida y ágil. Y vinculado con esto, cómo evaluaría la situación, cómo la calificaría, si se va avanzando positivamente o todavía tenemos que esforzarnos en esto mucho más, en la superestructura que existe de colaboración y cooperación a nivel de la Unión Europea y, cómo no, la que pueda haber a nivel mundial de cooperación de los países a la hora de una defensa común de ciertos aspectos que no controlan, porque los que controlan los va a controlar el que tenga capacidad de ese control, y nunca los va a poner a disposición de ningún otro. Esto que ha comentado de China no es una banalidad; no solo está hecho para defenderse, sino probablemente también para otro tipo de objetivos y misiones, como de hecho parece ser que se puede desprender, y no porque esté el Estado implicado, porque no se sabe o no se quiere plantear como una concreción definitiva, pero algunos países de los que provienen muchos ataques sí identifican de dónde vienen en cuanto a zonas geográficas, regiones y zonas, como es el caso de la propia China, algunos países de la ex Unión Soviética o de la propia Federación Rusa o de algunos expaíses del antiguo bloque del este. ¿Cómo evaluaría esta cooperación a nivel mundial, y por supuesto la de la Unión Europea, que es con la que tenemos más cercanía y hay más fiabilidad y confiabilidad a la hora de establecer esos mecanismos de cooperación?

Muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señor Raffo.

Por el Grupo Popular tiene la palabra la señora Vázquez.

cve: DSCG-12-CM-126

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

Quiero dar la bienvenida y agradecer la intervención del señor Cavanillas, de la empresa Atos. Ha sido muy práctica. Y quiero felicitarle sobre todo porque ha tocado algunos extremos que hasta estos momentos no habíamos valorado, como puede ser la implicación que tiene la ciberseguridad para las pymes y para los autónomos, que efectivamente no tienen recursos. Hoy hablaba usted aquí de copago y habría que ver qué posibilidades habría de actuación por parte de las comunidades autónomas o del propio Gobierno de España.

Tenemos claro que la economía digital es un hecho, que es una revolución que está ahí, y que no podemos quedarnos atrás en esta revolución, y menos por miedo a ser atacados. España a día de hoy no está entre los diez mejores países en ciberseguridad, nos adelantan países como Estonia, Canadá o Georgia. Creo que tenemos una media en el último año de 130 000 ciberincidentes, es decir, estamos hablando de una cantidad muy importante. Según algunas estadísticas la ciberseguridad en España, a raíz del WannaCry, pero ya antes, estaba siendo un problema que asumían las empresas y el Gobierno. A día de hoy la industria de ciberseguridad en España ha crecido un 10 %, mucho más que la media europea, lo cual hace ver también la conciencia que en España estamos teniendo —que no es suficiente— sobre la ciberseguridad. Los usuarios de Internet debemos tener seguridad y confianza. En este mundo en el que las transacciones electrónicas superan muchas veces al pequeño comercio, al comercio tradicional, los usuarios tenemos que tener confianza en esas aplicaciones y en toda esta revolución digital. Y nosotros, en este caso como legisladores, tenemos que intentar dar esa confianza y esa seguridad, pero es cierto que el tiempo ciber es mucho más rápido que nosotros. Posiblemente cuando finalicemos esta ponencia y sus conclusiones, que creo que será ya próximamente, antes del mes de junio, muchas de las cosas que aquí hayamos propuesto estarán ya desfasadas. Leí un día que solo un 24 % de las empresas españolas son eficientes cibernéticamente. Este es un problema. A lo mejor usted tiene un dato más actualizado, pero un día aquí nos hablaron de un 24 %, lo cual me parece un número escaso.

Hoy venían hablando de *hackers,* y veo que aquí hay ferias de *hackers* y que vamos a ver quién hace mejor este concurso, y a mí esto me da un poco de temor. Se organizan desde los ministerios y desde Europa estas grandes actuaciones para ver en qué lugar queda España, y creo que hemos quedado entre los primeros en Europa en ejercicios de *hackers*, pero pienso que no debemos olvidar que un *hacker* es una persona que entra en mi casa sin previo aviso, que investiga mi casa, y eso es un delito. Entonces no sé si nos estaremos equivocando a la hora de hablar de los *hackers*. Usted decía cómo un *hacker* podía ser un tigre incluso contra la propia empresa o el propio ministerio que lo contrata. No sé qué le parecen a usted este tipo de eventos y hasta dónde podríamos poner nosotros un límite en esta captación que se hace ahora. Está de moda y dicen que España necesita 30 000 personas en ciberseguridad, y no sé hasta qué punto estas ferias o estos concursos están siendo una buena manera de captar. Usted hacía referencia a los policías, yo soy de profesión inspector de policía, y cuando le das una pistola, un arma a un policía tienes que saber cómo la va a usar, y nosotros a lo mejor estamos metiendo al zorro a cuidar de las gallinas, sin saber quiénes son los zorros.

Me gustaría hacerle una serie de preguntas. Una de ellas es cómo valora usted la colaboración público-privada en materia de ciberseguridad en España y en Europa. Respecto a la Directiva NIS sabe que estamos ahora en fase de enmiendas, y le pregunto qué propondría usted al legislador como modificación de ese decreto que ha transpuesto la Directiva NIS. Respecto a lo de la captación del talento cómo propone usted que podríamos captar talento en materia de ciberseguridad. También me gustaría saber, ahora que el Gobierno va a aprobar el impuesto a las tecnológicas y la tasa Google, cómo cree que esto puede afectar a un usuario, como por ejemplo a un comprador a través de Amazon; si cree que los impuestos a las tecnológicas van a mejorar la seguridad de las plataformas que usamos habitualmente, algunas de carácter gratuito. Nosotros aquí estamos hablando sobre la ciberreserva que tienen Holanda, Reino Unido, Alemania y Estados Unidos —llámese ciberreserva o un colaborador de ciberseguridad—, y usted ha hecho referencia a un ejército de la red; nosotros nos estamos refiriendo como a la reserva del ejército. ¿Cómo valoraría usted crear una ciberreserva? Sería para gente voluntaria, aunque no con carácter altruista, sino con ciertas compensaciones: nosotros en su momento valorábamos, aparte de las compensaciones económicas, tener una puntuación para acceder a puestos de la Administración o tener un currículum mejorado y valorado para ir a algunas empresas a trabajar; la propuesta estaba un poco en el aire. Después, sobre el intercambio de información entre los CERS autonómico y estatal, ¿cómo lo valora usted? ¿Es suficiente o deberíamos mejorar el tipo de información? Y también querría que nos

cve: DSCG-12-CM-126

dijera cómo impulsar la industria española de la ciberseguridad, que es un problema que también queremos abordar. Por último, si considera que debemos regular de alguna manera la identidad digital.

Yo soy una amante de las redes, me encanta usarlas, pero ahora estaba viendo aquí un tuit que ponía: Ojalá su madre hubiera cerrado las piernas cuando nació, hija de puta. Yo no sé quién es ese señor y esto lo estaba leyendo ahora mismo. Esto es todos los días así. ¿Cómo cree usted que deberíamos regular la identidad digital? Porque lo que me estoy planteando es cerrar mi cuenta de Twitter, y por lo tanto gana la batalla la gente mala. Usted debería aconsejarnos algún tipo de regulación respecto a la identidad digital, porque yo sí digo que creo en la libertad, y me pondría a debatir en las redes, pero no sé con quién estoy debatiendo muchas veces.

Nada más y muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, señora Vázquez.

Nuevamente le damos la palabra al señor compareciente para dar respuesta, en la medida que considere oportuno, a las intervenciones de los representantes de los grupos parlamentarios.

El señor **CAVANILLAS DE SAN SEGUNDO** (chief big data & security officer, responsable de ciberseguridad de la empresa Atos): He apuntado todas las preguntas y esto me llevará siete horas o siete horas y media. **(Risas).** Voy a intentar ser breve en mis respuestas. Algunas preguntas están ligadas unas con otras, así que les intentaré responder por manojos, digamos.

Empiezo con las del señor Yanguas, del Grupo Mixto. ¿Cómo se implanta un SOC para pymes, por ejemplo, en Navarra? Bueno, lo primero es saber qué es un SOC, que es la primera reflexión para aquellos que no estén metidos en este mundo. Un SOC es un centro operativo de seguridad; es un grupo de personas —cinco, diez, quince o veinte personas— que tienen delante unas pantallas que están vigilando todo lo que pasa en las redes de aquellos a los que el SOC vigila. Si es una gran empresa, por ejemplo, una empresa de energía, el SOC puede estar compuesto —y este es un caso exacto— por dieciséis personas que vigilan todos los servidores de esa empresa de energía, los ordenadores que controlan la producción, transmisión y recepción de esa empresa de energía, y en cada momento evalúan en cada subsistema los problemas que está habiendo de forma descriptiva, es decir, los problemas hasta hoy; de forma predictiva, es decir, con lo que está llegando qué es lo que va a pasar, si ha comenzado un posible ataque; y de forma prescriptiva, es decir, dado que ya sabemos que va a haber un posible ataque en los próximos diez minutos, qué acciones debe tomar esa red para cerrar determinados puertos o para atacar o defenderse de determinadas maneras. Son importantes las tres partes: descriptiva, predictiva y prescriptiva.

Es importante que estas personas conozcan una herramienta de gestión de eventos, una herramienta SIEM, y que estén encima y de forma permanente 24x7 vigilando esos sistemas. Para una gran empresa, como la que acabo de describir, estamos hablando de dieciséis personas, pero si en vez de ser una gran empresa son cien pymes, digamos que son cien subredes que hay que vigilar y analizar de forma descriptiva, predictiva y prescriptiva. Así pues uno puede tener un taller y puede recibir una llamada a las dos de la mañana del SOC de las pymes, diciendo: oye, tú no lo sabes, de hecho estas durmiendo, pero alguien está entrando en tu ordenador. Lo hemos frenado y hemos parado un ataque, pero hace falta meter una *password* para volver a iniciar el ordenador, lo digo por si quieres iniciarlo ahora o mañana por la mañana o lo que sea. Alguien está vigilando tu casa, vigilando tu sistema. Eso es un SOC. Pero claro, hay que pagar esos dieciséis sueldos, y hay que pagar las herramientas informáticas, y son sueldos más las horas extras de los fines de semana y de las noches; o sea, hay un coste importante y ese coste una pyme no lo puede hacer. Yo no puedo pagar a dieciséis personas con lo que saco de los coches. Yo necesito que muchos más talleres paguen cada uno un poquito para poder financiar eso. Y el Estado o las comunidades autónomas —y no voy a meter el origen del dinero, pero la pyme no, la pyme puede pagar hasta aquí y todo lo demás lo tiene que pagar alguien— deben tener un sistema que vigile la infraestructura que mi pyme y todas las pymes relacionadas conmigo territorial y sectorialmente tienen.

¿Cómo implementarlo? Pues se llama a cualquiera de las muchas —la mía es una, pero hay muchas más— que dan servicios de SOC y proporcionan este servicio. Y hay más cosas, no solo SOC; también hay otras cosas: antivirus, protección de *endpoint*, etcétera. Hay distintas herramientas que deben alinearse para proteger a los grupos de pymes. Curiosamente yo esto no lo he visto. Antes de venir a esta ponencia he analizado en cada comunidad autónoma si había algún tipo de agrupación de pymes que se hubiera puesto de acuerdo para protegerse en Murcia, en Navarra, en la isla de El Hierro, me da igual; no he visto ninguna. No tengo la certeza de que no existan, pero si yo, que estoy metido en el mundillo, no

cve: DSCG-12-CM-126

me he enterado, el del taller tampoco. Quiero decir que si alguien está haciendo algo no sé quién es; creo saber el cien por cien de los SOC que hay en España, al menos los privados, creo conocerlos; ninguno es de uso colectivo por parte de las pymes, y si lo hay yo no lo conozco. En cuanto a cómo se implanta una SOC, esto es lo que se haría.

El señor Salvador, de Ciudadanos, me ha preguntado sobre la formación del usuario final y cómo sería abordar el tema de las grandes academias de formación, que está ligado con la pregunta de la señora Vázquez, del Grupo Popular, sobre la captación de talento y cómo hay que gestionar esta captación de talento, y alguien más que me ha preguntado sobre esto, incluso sobre los eventos de *hackers* en los que invitamos a la gente. Yo no sé si el problema está en dar demasiada información o no. Le voy a poner un ejemplo específico, de hecho de ayer martes 22 de enero. Ayer, un niño de catorce años le dijo a su profesora: ¿sabes qué quiero ser de mayor? Sicario. La profesora alucinó y dijo: te estás equivocando, no sabes lo que quiere decir esa palabra. Y dijo el niño: sí, sí; si me meto en Internet profunda sé dónde encontrar las armas para comprar. La profesora le dijo a los niños de alrededor: pero esto que está diciendo este niño está de broma ¿no? Y le contestaron: ¡no, no; si nos ha enseñado la Internet profunda, si hay violaciones! Pero vamos a ver, este niño con catorce años está accediendo a una información a la que no se debería acceder; se puede, pero no se debe. Teóricamente la ley solo te condena si cometes algún delito. Este niño todavía no ha cometido nada, pero por el camino que va… ¡Menudo camino lleva! El problema no es tanto si saber o no —porque si tú te vas a Google y pones Internet profunda empiezan a salir, tengas la edad que tengas, todas las cosas que no deberías mirar—, sino si realmente el niño tiene la intención de hacerlo.

Me voy a ir un momento al mundo físico. Si un niño de catorce años quiere ser un asesino, se va a la cocina coge un cuchillo y mata. ¿Debemos esconder los cuchillos o debemos educar a los niños de catorce años en que eso no hay que hacerlo? A un niño de tres años sí, pero a un niño de catorce años no se le pueden esconder los cuchillos; en la cocina hay cuchillos, hay que cortar el jamón. El problema es que no está habiendo asesinos todos los días en todas las casas porque los niños de catorce años saben que, aunque el cuchillo esté ahí, no se utiliza para eso. Una cosa es poder comprar un arma, otra es poder ser un sicario, y otra es querer ser un sicario. Entonces, ¿debemos cortar los eventos de *hackers*? ¿Debemos impedir que la gente acceda a la información de cuáles son las formas de atacar en el mundo de la ciberseguridad? No lo sé. Así muy conveniente no parece; no me parece demasiado atractivo que los niños encuentren dónde está la Internet profunda, por dónde te van a atacar, cómo comprar armas o cómo comprar otras cosas. No me parece muy conveniente, pero mi opinión la quiero ligar estrictamente al mundo de la tecnología. No quiero entrar en una opinión social, porque es que esto ya no es un tema tecnológico, es un tema de en qué debemos formar a los niños y en qué no. Y si hemos llegado a que a un niño —es uno de miles— le apetezca ser un sicario, porque mola, y no le apetezca ser político, banquero, empresario, sacerdote, etcétera, porque todas estas profesiones están muy denostadas en los medios de comunicación todos los días; están denostadas denostadas las grandes profesiones que construyen la sociedad, y de algún modo una profesión que por defecto es lesiva para la sociedad, ¡es la que mola! Y además voy a ver en Internet cómo hago para ser eso. El problema no es un problema cibernético; es un problema de personas, es un problema social.

¿Se debe cortar la información? Yo creo que hay que segmentar la información técnica en varias partes. La primera es: la información técnica muy exacta y muy concreta para formar tigres —para formar *hackers*— que sirvan al Estado y a la empresa debe ser igual que si alguien pide permiso de armas. Tiene que hacer un curso, tiene que ir a una academia y no es algo que deba publicarse de forma notoria. Sí se debe extender —y para mí esto es importante— una serie de consejos a la población de qué cosas no hacer con el móvil, en qué condiciones hay que vigilar siempre el móvil de los menores y de los mayores y tener a tus personas cercanas informadas de qué peligros tiene el ciberespacio. Y esto es mucho más que estos dos minutos de charla. Hay demasiados peligros en el ciberespacio. Creo que los centros de día que tan buen rol tienen en muchas comunidades autónomas y muchas ciudades, además de entretener a los mayores, deben incluir cursos específicos y formación para que cuando te llegue al *mail* que el banco te está diciendo algo lo ignores porque el banco no se comunica así. O que si alguien te está diciendo: «Hola, me llamo Puri, estoy buscando pareja y también tengo setenta», y no sabes quién es Puri, te plantees que Puri es un señor de Rusia con bigote. Tienes que tener mucho cuidado al conectarte con alguien, y no solo en los colegios sino también en los lugares donde se encuentra la tercera edad. Ya en el mundo de los discapacitados ni entro porque es demasiado grande.

cve: DSCG-12-CM-126

Creo que hay que segmentar información exacta para ser *hacker*. En los centros donde se enseña a disparar pistolas y a ser un *hacker* hay información de protección ante los ataques. Había una pregunta del Grupo Socialista sobre si estar en un ejército de la red o en una actividad cibernética es para defendernos o es para atacar. Volviendo al mundo físico, nuestro ejército no solo compra chalecos antibalas, también compra ametralladoras. En algún momento habrá que matar al enemigo o al menos dispararle. No veo descabellado que nuestros tigres —los de nuestro ejército de la red o de nuestras empresas privadas, lo veo con mayor *endorsement* desde el punto de vista legal en el ejército de la red— disparen a quien tengan que disparar. Si yo veo un grupo de delincuencia organizada que está atacando un pantano mediante determinadas cosas y está a punto de provocar una catástrofe que puede matar 'n' personas, no veo descabellado que nuestros tigres desarmen su sistema informático para que no puedan ejecutarlo. Es lo que hay que hacer, para mí no es una opción sino nuestro deber, disparar en ese sentido para proteger a los ciudadanos. No lo veo descabellado, por eso damos pistolas a nuestros soldados porque hay que disparar y en la guerra es lo que hay que hacer. ¿Es bueno hacerlo? Hombre, no con mucha frecuencia. Hay que entrenarse en campos de tiro y hay que saber hacerlo, pero hay que tener personas preparadas para atacar los sistemas del enemigo, por supuesto.

Sobre la actividad de China, Rusia y Unión Europea, no todo lo que es chino es del Estado chino. No sé si conoce usted el país en profundidad. Afortunadamente he estado seis veces allí y hasta he estudiado dos años de chino y, según mi conocimiento de su cultura, me da la impresión de que, una vez que cayó el régimen anterior, la reacción de la gente ante un sistema que intentaba que todo fuera transparente y el Estado tenía que saberlo todo es que ahora todo el mundo oculta lo que hace. Nadie sabe lo que hace el vecino y el Estado no sabe nada de lo que hace nadie. Cuando dicen que la economía china ha crecido un 8%... No, lo que el Estado chino sabe de la economía china es que ha crecido un 8%, pero ¡vete tú a saber lo que ha crecido la economía china! La ciberactividad que procede de China, la que procede del Gobierno o de su ejército será la que sea y el resto es de iniciativa privada china que va a su bola y a su velocidad. Pasa lo mismo que en Rusia; en la Federación Rusa tienes una serie de grupos no necesariamente legales, no alineados con el Gobierno —o sí— que hacen una serie de cosas y que el Gobierno no controla. Lo mismo sucede en Georgia, en Armenia, en Kazajistán, en todos los antiguos países pertenecientes a la Unión de Repúblicas Socialistas Soviéticas.

En Europa es un poco diferente. Me ha preguntado usted: ¿cuál es su evaluación de la estructura de la Unión Europea desde el punto de vista de ciberseguridad? Mi evaluación es la misma que con todas las demás estructuras de la Unión Europea, y hablo como ciudadano europeo: ¡Es 'mu' flojo! Como Unión Europea, ¡es 'mu' flojo! Estamos muy poco unidos, parece que estamos unidos pero cada uno tiene una estrategia, hay que cambiar legislación. ¡Anda que no cuesta hacer una directiva y, cuando la directiva sale, anda que no cuesta que los Estados hagan sus leyes! No parece que estemos muy unidos ni para esto ni para nada de lo demás. Sí me creo la GCA, la Global Cyber Alliance, la Alianza Cibernética Global, que nació hace más de un año y en la que ya está incluido el Grupo de Defensa de los Estados Unidos de América, se ha apuntado la Policía de la ciudad de Londres y hace unos meses —creo que fue en septiembre— la Europol también se ha apuntado. Pero si usted me pregunta cuál es la conexión entre la Europol y la Policía Nacional española o la *Gendarmerie* francesa, pues alguna hay pero son cuerpos distintos que se coordinan; no actúan de forma integrada, se coordinan. ¿En qué medida tiene sentido que una dispersión o diversidad de organizaciones actúen en el mundo de la ciberseguridad teniendo en cuenta que en el mundo de la ciberseguridad hay que tomar decisiones en minutos? Pues la existencia de muchas organizaciones no es positiva. Lo mejor es crear estructuras de decisión unidas y cuantas menos y más integradas estén las instituciones, mejor. Yo hablaba de integración en una estructura supranacional de nuestras estructuras, pero dividir nuestras estructuras en más no lo veo muy positivo, y no porque yo sea contrario a la multiplicidad de estructuras sino porque realmente en el mundo cibernético una hora es muchísimo tiempo. Hay que tomar decisiones, hay que actuar, hay que parar, hay que disparar y para eso hay que tomar decisiones a mucha velocidad.

Tengo muchas preguntas del Grupo Popular, una pregunta importante del Grupo Ciudadanos y varias de Unidos Podemos que me gustaría responder. Galicia. Quizá no soy yo la persona. No me sé de memoria —debería— todos los proyectos del grupo Atos en la historia. Creo recordar que el proyecto de Galicia —si no me equivoco— fue de año y medio entre 2015 y 2016, fue un éxito, conectó el sistema gallego de salud con el sistema de Estados Unidos, trabajó mucho los datos sanitarios y fue una experiencia interesantísima y recibimos felicitaciones de mucha gente. Estamos en 2019, ahora mismo hay otra estructura de datos. La Ley Orgánica de Protección de Datos existe todavía pero la GDPR ha comenzado en mayo de 2018 y ahora

cve: DSCG-12-CM-126

mismo hay muchos más planteamientos. ¿Es distinto el dato médico de otros datos? No necesariamente. Es importante, como lo son otros datos, pero mi cuenta corriente es importante. ¿Tiene una gestión distinta? Pues no debería tratarse ni publicarse con alegría. ¿Funciona bien el sistema sanitario español? Diría que no y voy a ser disruptivo aquí. Si voy a un médico —voy a escoger un tema sensible— de enfermedades de transmisión sexual y me siento en la sala de espera y sale una enfermera y ante veintisiete personas dice: ¡Señor Cavanillas! Hay veintiséis personas que han oído mi apellido ligado a que estoy yendo a un experto en enfermedades de transmisión sexual, pues igual no es buena idea que digan en voz alta mi apellido. Vamos, y no me meto en el mundo cibernético, pero cualquier de los veintiséis puede decir: pues he visto a este que estaba en la consulta de esta especialidad.

Eso sí, la persona que me ha consultado, esa persona que está tuiteando esto, no sé quién es. Efectivamente, me dan ganas de cerrar Twitter y decir que hay una serie de personas que me están atacando que no sé quiénes son y que debe haber alguna manera de que llegue hasta ellas. Y esto está ligado a otra pregunta sobre en qué medida se está avanzando en la identificación de los ordenadores o personas que trabajan en Twitter. No creo que se pueda llegar ni a corto ni a medio plazo a la identificación automática ni de las personas ni de las máquinas que actúan en Internet. ¿Por qué? Y esto sí es una respuesta técnica. En primer lugar, no todos los Estados de la tierra tienen la misma legislación en cuanto a gestión de redes. Hay muchos Estados en los cuales puedes tener una cuenta en Internet, dices en voz alta que te llamas Mohamed —y digo un nombre al azar—, no te llamas Mohamed pero nadie lo confirma y tú te conectas y eres Mohamed. En el momento en que eres Mohamed, estás conectado en algún sitio y ya desde allí nadie puede saber quién eres, aunque seas de Murcia, desde Murcia te conectas con ese país, dices que eres Mohamed y actúas como Mohamed. Nunca sabrá nadie que eres un tío de Murcia. Por otra parte, si todos los países se pusieran de acuerdo, tuvieran la misma legislación y confirmaran uno por uno todos los teléfonos móviles, todas las *tablets* y todos los ordenadores, aun así hay otra manera técnica de evitar que te identifiquen y es utilizar la Internet profunda. ¿Cómo funciona la Internet profunda —lo explico en medio minuto—? Hablando de la Internet que se ve, la parte de Internet que todo el mundo ve, Google o Amazon, puedes ir a Amazon y escribir que quieres comprarte un paraguas. Y lo que te responde es un ordenador de Amazon que todo el mundo sabe dónde está, que es un ordenador concreto que está ubicado en Alcobendas y que está respondiendo a otro que hay en Londres, que todas las horas del día tiene esa foto de ese paraguas y tú puedes conectar a las dos de la mañana y te da la orden de enviarte el paraguas a tu casa. Veinticuatro por siete, es el mismo ordenador dando la misma página. Si tú quieres comprar una ametralladora —tienes catorce años, pero quieres comprar una ametralladora— en la Internet profunda, la tienda de ametralladoras no puede estar en Alcobendas veinticuatro por siete porque la pillan. Entonces, ¿qué es lo que hace? Está treinta segundos en un ordenador, un minuto en otro ordenador, treinta segundos en otro ordenador, y tú tienes un *browser*, un explorador de Internet, que está conectado a los cambios y tú solo ves la página web, pero la página web está bailando para evitar que la pillen. A lo mejor treinta segundos está en el Ministerio de Industria, pero nunca se sabe porque ha aterrizado en la página web y luego se ha ido. Esa manera tan rápida de cambiar, que es como funciona la Internet profunda, lo que hace es evitar mediante todos esos cambios que la puedan perseguir. Pero es que pasa del Ministerio de Industria de Madrid a un ordenador en Kazán, en Rusia, y lo siguiente es uno en Argelia, y lo siguiente uno en Alberta, Canadá. Tú no lo ves, pero está pasando por debajo y técnicamente es sumamente difícil de encontrar. A medida que vayamos teniendo mayores infraestructuras tecnológicas, mejores y más rápidos ordenadores y mejores y más rápidos sistemas de telecomunicación irá más rápido, no va a ser nada fácil. Y en el momento en que haya un solo punto en la red, uno solo, en el que puedas dar opacidad a tu persona —Mohamed— ya da igual. Tú haces siete saltos, uno de los siete es Mohamed y a partir de ahí ya nadie puede trazar para atrás, y sigue siendo el mismo señor de Murcia.

Yo creo que hay que trabajar en las personas. Al final, detrás del problema cibernético, que es grande, hay personas. Nosotros poco a poco iremos avanzando hacia la tercera edad —algunos estamos más cerca y otros más lejos— pero a nuestros jóvenes les estamos dando demasiada información en cuanto a tecnología y, sin embargo, no estamos formando su espíritu, su motivación, hacia dónde debe encaminarse. Ningún niño de catorce años, aunque no existiera Internet, debería pensar que de mayor quiere ametrallar gente, porque eso no apetece, no debería apetecer. Eso no es un problema cibernético.

En cuanto a las relaciones público-privadas, cuál es el éxito o no de las mismas y si los mecanismos que hay son buenos o no, en España yo creo que las relaciones dentro del mundo público y entre las instituciones están bien gestionadas desde el punto de vista cibernético, sobre todo gracias al CNPIC. Hay un SOC para la Administración pública —no sé si lo sabéis— que lleva el CNPIC, con lo cual si tienes un

cve: DSCG-12-CM-126

problema en la Administración pública tú llamas a ese SOC y te pueden resolver tu problema, pero no está ligado al mundo privado. En el mundo privado no hay intervención por parte del Estado. Sí, hay recomendaciones, pero nada que nos ayude por parte del Estado a resolver nuestros problemas de ciberseguridad. A nosotros en Atos no nos afectó WannaCry porque ya estábamos muy blindados mucho antes de que llegara WannaCry. Algunos de nuestros clientes sí fueron afectados por él, a muchísimas pymes les afectó. Lo que el Estado hace es recomendar. De hecho, una de las cosas que planteo es: no recomendéis, tenéis que financiar, blindar las pymes y cambiar esto. Pero no porque exista un abandono del Estado hacia la empresa privada sino porque el enfoque del Estado hasta ahora ha sido: yo tengo una función pública y mi función pública es poner semáforos, poner policía, pero mi función pública no incluye algo que las empresas deberían buscarse por su cuenta. Igual que si tú tienes un niño y le tienes que vestir, ya le comprarás tú el pantalón. ¿Debe cambiar este enfoque? Yo creo que sí y creo que debe ser en base a copago. Hablábamos sobre si es discutible o no esta manera. Yo creo que debe ser en base a copago. ¿Por qué lo creo? No creo en los servicios gratis; el problema de los servicios gratis, que son muy bienvenidos cuando no tienes dinero y eres una pyme comenzando, es que son susceptibles de fraude. Te he hecho un servicio de ciberseguridad y tú pagas un poquito; no pongas que es uno, pon que son siete. Total, a ti te da igual porque es gratis y yo cobro siete veces eso, te dice el proveedor. Ese tipo de fraudes —y hay más, este es uno de los muchos— se evita porque si tengo que pagar 50 euros por una llamada ya me cuidaré muy mucho de decir que te he llamado siete veces; te he llamado una y yo te pago tus 50 y los otros 150 la comunidad autónoma. Pero, claro, esa llamada son 200 euros. El estar a las dos de la mañana, el tener ese conocimiento y el tener esa herramienta activa no es gratis, pero yo pago mis 50 y los otros 150 que los pague el Estado, la comunidad autónoma o quien sea que tiene dinero, que no es la pyme. ¿Funciona hasta ahora? Pues hasta ahora dan recomendaciones, sí nos defienden nuestras infraestructuras críticas, las que nos afectan. Seguimos teniendo Internet, seguimos teniendo luz, no se ha desbordado ningún pantano, por ahora va todo bien, los Juegos Olímpicos van bien —esto no es público—, y los desastres que estamos teniendo en el mundo de la ciberseguridad están teniendo impacto a pequeña escala pero no a gran escala. ¿Debería haber más? Sí, sí, sí.

El Grupo Ciudadanos me preguntaba por las grandes academias de formación. Para mí las grandes academias de formación son como la academia de Policía, diferentes, porque no eres policía al final, pero son cuatro o cinco años, entre los dieciocho y los veintitrés, en los que tú sales con un título pero que no es ingeniero de no sé qué o licenciado en Físicas, sino: he sido formado en las tecnologías, me ha costado mucho entrar en esta escuela, me he dejado los cuernos, conozco formación, si no militar, al menos policial, conozco los peligros, sé entrar en la Internet profunda, he experimentado lo que es Internet profunda, he entrado, he atacado, sé dónde encontrar a los pederastas, sé dónde se trafica con droga y he ayudado al Estado a hacerlo durante cinco años. Pues bien, en los próximos cuarenta mi vida profesional será ayudar o bien al ejército en la red o bien a las empresas a luchar contra ellos, pero no voy a ser tan idiota de quebrar mi carrera profesional a los veinticinco pasando a ser un sicario. ¿Por qué? Porque estoy quebrando lo que ahora mismo percibo como mi carrera profesional que son cuarenta años. Ese escenario futuro no se produce hoy. Hoy lo que se produce es un chavalín cuyo objetivo en la vida no va mucho más allá de ser participante de *Mujeres y hombres y viceversa* o poco más, que está viendo en la televisión que son todos unos corruptos, que los políticos, los banqueros, los empresarios son todos unos sinvergüenzas y piensa: pues yo también. Y no tiene una base ética en la que trabajar así que piensa: pues aprendo un poco de Internet en un año o año y algo y a ver qué pillo. Eso es lo que hay hoy. Eso tiene que cambiar y tiene que hacerlo radicalmente. Ni ese chaval debe acceder a información puntera sobre cibertecnología ni tenemos que permitir que nuestra juventud tenga esos colectivos. Tenemos que dar una formación. No me parece mal lo de las seis empresas de China. Yo pondría una muy grande en Madrid, una muy grande en Barcelona, una muy grande en Canarias, una muy grande en Galicia y para poder entrar en esa facultad te dejas los cuernos para sacar las notas y estás cinco años y sales como uno de los —muy pocos, 50 000, 60 000 en España— tigres oficiales que pueden entrar en el ejército de la red o en las empresas privadas. Eso es lo que hoy no tenemos y deberíamos tener.

Creo que he respondido a todo.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, don José María Cavanillas, de la empresa Atos, por las respuestas.

Vamos a dar nuevamente la palabra a los portavoces de los grupos por si quieren añadir algo. Luego, nuevamente, le daremos la palabra para cerrar.

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

cve: DSCG-12-CM-126

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

Intervengo brevemente para agradecerle de nuevo su comparecencia y por haberme respondido a la única pregunta que le he hecho.

Muchas gracias. Buenos días.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señor Yanguas.

Por el Grupo Ciudadanos, señor Salvador.

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

También quiero felicitarle, evidentemente. Como ya he dicho, suelo intervenir más en esta Comisión y como usted ha sintetizado tanto y ha aportado algo tan importante he intervenido poco, como voy a hacer ahora. En la parte final, con respecto a lo que ha dicho, estoy totalmente de acuerdo —repito— con todo su planteamiento y también con el planteamiento con respecto a los jóvenes. Uno de los grandes problemas en este momento es que la figura del *hacker* se está prestigiando, porque parece que ser *hacker* es ser un poquito más listo que la media y que consigues hacer cosas importantes y al final, incluso, te pueden contratar y eso también es una vida para buscarte un plan B, para poder ser una persona importante. Y en el camino tú ya decidirás qué es lo que quieres hacer con eso. Creo que estamos hablando de una cuestión que tiene que ver con valores, por lo de los cuchillos. Esto tiene que ver con valores y la cuestión es qué quiero ser de mayor: quiero rescatar a niños que se caigan en pozos, quiero salvar a las personas siendo bombero, quiero ser policía, quiero ejercer la ciberseguridad porque es algo que me gusta, domino la tecnología y por tanto me puedo sentir cómodo en ese puesto de trabajo y eso me puede hacer sentir motivado. Es una cuestión de valores, de motivación y la parte que resalto de usted, y que ha aportado certeramente, es que hacen falta los instrumentos para formar ese tipo de personas para que puedan tener ese tipo de oficios, donde se prestigie esa labor y que esa labor, según vas aprendiendo, vaya acompañada también de valores para que al final no tengas que decidir si me voy al sector privado de los buenos o al sector público de los buenos o incluso, como he aprendido mucho, me voy al de los malos. Un matiz, que sé que usted lo habría dicho perfectamente: el gasto en ciberseguridad es un ahorro del enorme gasto que genera la inseguridad y todos los efectos que está provocando. Por lo tanto, respecto a que las administraciones tienen que intervenir, comparto con usted el concepto del copago para darle una buena racionalidad y que se haga lo que realmente es importante y se consigan objetivos. Estamos hablando de que las pérdidas son enormemente millonarias si no se hace absolutamente nada, por lo que no podemos estar al margen.

Nada más que decir a su impecable intervención.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, señor Salvador.

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

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Intervengo brevemente solo para agradecerle su intervención. Estoy segura —precisamente porque ha sido tan propositivo— de que interactuaremos después de hoy alguna vez más para pedir aclaraciones cuando nos revisemos todas las propuestas de cara a nuestro informe. Ha sido clarísimo y práctico. No tengo nada más que agradecerle su participación.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, señora Angustia.

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

El señor **RAFFO CAMARILLO:** Simplemente quiero darle las gracias por las respuestas. Han sido muy concisas, directas y claras, al igual que su primera intervención. Agradezco su presencia porque así nos enriquecemos todos a la hora de trabajar en una causa común.

Muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señor Raffo.

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

La señora **VÁZQUEZ BLANCO:** Muchas gracias.

Quiero agradecer al compareciente las explicaciones y las respuestas a las preguntas de manera tan clara y concisa.

Muchas gracias.

cve: DSCG-12-CM-126

El señor **VICEPRESIDENTE** (Jiménez Tortosa): tiene usted la palabra por si quiere añadir algo.

El señor **CAVANILLAS DE SAN SEGUNDO** (chief big data & security officer, responsable de ciberseguridad de la empresa Atos): Quiero agradecerles, en primer lugar, haberme dejado venir aquí a hablar como responsable de ciberseguridad. Y como ciudadano: ¡a ver qué hacéis! **(Risas).** A ver qué pasa en esta Comisión y si mi país cambia no ya por lo que he dicho yo —que ha sido un poquito—, sino por todo lo que han dicho los comparecientes anteriores.

Muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias por su comparecencia. Ha caído muy bien y ha sido muy realista.

Muchas gracias. **(Pausa).**

— DEL SEÑOR BERMÚDEZ GONZÁLEZ (FISCAL DELEGADO ADSCRITO AL SERVICIO DE CRIMINALIDAD INFORMÁTICA DE LA FISCALÍA GENERAL DEL ESTADO), PARA INFORMAR CON CARÁCTER GENERAL SOBRE LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/001895 y número de expediente del Senado 713/001135).

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Señorías, continuamos porque vamos con bastante retraso.

Damos la bienvenida a don Jorge Bermúdez González, fiscal delegado adscrito al servicio de Criminalidad Informática de la Fiscalía General del Estado. Agradecemos su atención de asistir a esta comparecencia para tratar de ilustrarnos en la medida de lo posible en este tema.

Muchas gracias por su comparecencia y le cedo la palabra.

El señor **BERMÚDEZ GONZÁLEZ** (fiscal delegado adscrito al Servicio de Criminalidad Informática de la Fiscalía General del Estado): Señor vicepresidente, señores componentes de la Mesa y señorías de ambas Cámaras, en primer lugar, para mí es un placer, un orgullo y un privilegio comparecer aquí en esta sede, la casa de la palabra, las Cortes Generales, habida cuenta de que hace ya poco más de doce años que juré precisamente ante la Constitución defender este Estado, esta nación, que se basa fundamentalmente en el Estado de derecho. Es un Estado social y democrático de derecho y, por ello, la Comisión de Seguridad Nacional, la que tiene que decirnos, prepararnos y darnos las directrices según las cuales debe dirigirse la política o la legislación orientada a defender este país, no puede ser más apropiada, es prácticamente justicia poética. Ahora bien, no quisiera que se lleven a engaño acerca de mi papel en esta comparecencia. Soy un fiscal de tropa, un fiscal adscrito a una fiscalía provincial, en este caso a la de Guipúzcoa, y evidentemente no soy el jurista llamado a explicarles a ustedes las cosas más complicadas de nuestra legislación porque para eso tenemos una fiscal de Sala del Tribunal Supremo que coordina la Unidad Central de Criminalidad Informática, doña Elvira Tejada, que además me consta que ha comparecido también en esta Comisión y que, en principio, es la que señala las líneas generales de actuación, sin perjuicio de que luego cada uno en el ámbito de su competencia en los casos que tenga que llevar adopte unas decisiones u otras, pero siempre procurando una unidad de actuación del ministerio fiscal, que es uno de los principios que rigen su actuación. En cualquier caso, las razones por las que entiendo que he sido convocado tienen más que ver con mi perfil profesional y personal en cierta manera, dado que la seguridad informática, la ciberdelincuencia y el combate contra estas formas de ciberdelincuencia y promover la ciberseguridad son dos de mis grandes pasiones de toda la vida desde que estaba en la universidad y, por supuesto, desde que ingresé en la carrera fiscal y, por ello, también, aparte de la fiscalía, tengo el placer de ser profesor en algún máster de ciberdelincuencia y haber sido convocado a algunas de esas reuniones de «*hackers*» —entre comillas— de las que hablaban antes, término que, lo siento mucho, está demasiado gastado por los medios y por la opinión pública para definir con precisión la clase de personas de las que estamos hablando. Les decía que creo que es mi perfil personal el que me lleva a venir aquí, dado que soy una persona dada al pensamiento lateral, lo que los anglosajones llaman el *thinking outsider the box*, pensar fuera de la caja, que se ocurran soluciones creativas, ya que la creatividad no siempre es algo que en la carrera fiscal o en la carrera judicial o en general en el mundo del derecho se tenga en especial estima.

Tenemos que remontarnos —siento en ese sentido ser un poco aburrido— a los orígenes del Estado de derecho. Como saben todos ustedes, el Estado es un constructo social, es una idea que surge a finales de la Edad Media cuando el feudalismo y el medievo llegan a su fin. Me interesa esto porque cuando

cve: DSCG-12-CM-126

estudié *Teoría Política* en la universidad nos explicaron que el feudalismo era un fenómeno en el que el poder económico accedía al poder político por accesión y basándose en un vacío de poder. Recuerden que cae el Imperio Romano, cae Roma, y hay una serie de señores terratenientes que tienen sus castillos, grandes extensiones de terreno, una población que depende de ellos, siervos de la gleba y mesnadas de caballeros que les defienden de posibles ataques y hay un imperio débil, un imperio que no puede extender su poder, es decir, no pueden decirles: Haz esto porque te lo digo yo. El imperio ha caído, no tiene esa fuerza. Siento decírselo, pero el Estado nación como lo conocemos está viviendo una segunda caída del Imperio Romano. A día de hoy existe un territorio en el que el Estado no puede extender los tentáculos de su poder como el Imperio Romano caído en aquel entonces tampoco pudo, y ese territorio es el quinto escenario que dicen los militares. Los tres primeros escenarios eran tierra, mar y aire, el cuarto escenario hace unas décadas se definió que era el espacio exterior y el quinto escenario es Internet, son las redes de telecomunicaciones, el ciberespacio, como prefieran llamarlo.

En el ciberespacio no hay un Estado que tenga un territorio propio. Ya nos lo dijo en 1996 en Davos John Perry Barlow cuando publicó su manifiesto de independencia del ciberespacio. Dijo que el ciberespacio es una cosa distinta, es un ente sin territorio y que, por tanto, los Estados debían mantenerse al margen de él. Y lo cierto es que no ha habido un Leviatán, como el que definía Thomas Hobbes. Me identifico mucho con Hobbes como filósofo porque él se definía como un liberal que tuvo miedo y yo, sin definirme como liberal, sí que tengo miedo, miedo de las cosas que pasan, de las cosas que me cuentan que pasan aquellas personas vinculadas con el aspecto técnico de la ciberseguridad y que me cuentan los problemas y las vulnerabilidades que hay. Porque no se llamen a engaño, señorías, la ciberseguridad es una disciplina transversal que abarca un montón de campos, desde la psicología, trabajar con los jóvenes, como ha dicho el anterior compareciente, la educación y, por supuesto, el derecho. Evidentemente, también la tecnología, la informática, tanto el diseño del *hardware* como del *software*, y las redes de comunicación, por supuesto, que son el núcleo central, pero si dejamos todas las demás disciplinas todo esto se convierte en una cuestión de ingenieros y parece que sobramos, y eso es lo que no se puede permitir. A este respecto siempre se está hablando de que hay un problema en este país a la hora de buscar talento en ciberseguridad. Lo he oído hasta en los medios de comunicación: El problema es buscar talento. El talento en ciberseguridad en este país, se lo voy a decir claramente, es como petróleo a flor de tierra en un campo de extracción petrolífera de Tejas a principios del siglo XX, está ahí y solo hay que rascar. Si tienen la posibilidad de acudir a una de estas convenciones de seguridad informática, donde lo único que se hace es una labor de compartir el conocimiento en una suerte de tregua olímpica en la que se pueden juntar de un lado gente del grupo de la Unidad de Delitos Telemáticos de la Guardia Civil, del Centro Nacional de Inteligencia con gente del colectivo Anonymous que, por supuesto, no revela su identidad como, por ejemplo, la famosa La Nueve de Anon, que es uno de los grupúsculos más activos en la actualidad, en ese momento nadie persigue a nadie, es una especie de olimpiada griega a la antigua usanza en la que existe una tregua tácita y en la que se comparte el conocimiento. Evidentemente, los que no acuden a esas convenciones, los que no revelan sus conocimientos, son los que tienen la intención de utilizarlos con fines llamémoslos antijurídicos o contrarios al Estado de derecho y bienestar de los ciudadanos, porque evidentemente no quieren que las Fuerzas y Cuerpos de Seguridad del Estado puedan tener acceso a eso que el resto de expertos en ciberseguridad les está contando.

¿Cuál es el problema entonces con el talento? El problema es retenerlo, no encontrarlo, porque la gente —siento decírselo— no trabaja a cambio de abrazos, sino de dinero. Tienen la mala costumbre de comer tres veces al día y pagar la hipoteca. En ese sentido, ¿quién tiene dinero? Todas esas grandes empresas tecnológicas englobadas en un acrónimo que se conoce como Gafam: Google, Apple, Facebook, Amazon y Microsoft, con algún otro advenedizo recién llegado como Twitter, que todavía no ha conseguido una monetización clara de su modelo de negocio y, por tanto, su continuidad ni siquiera está garantizada de aquí a unos años y mucho menos a unas décadas. Estas empresas sí tienen ese capital, sí tienen este poderío económico y sí que pueden permitirse pagar lo mejor que el dinero pueda comprar, el mejor talento y no solo las mejores herramientas, porque en lo que llamamos la sociedad del conocimiento, como se pueden imaginar, el activo más valioso, y perdónenme la obviedad, es precisamente el conocimiento. Estamos hablando de ciberarmas y de ciberejércitos. Las ciberarmas no son programas de ordenador, eso son las municiones. Las ciberarmas son el informático que tiene esos conocimientos y sabe que este sistema funciona mal y puede ser atacado a través de esta vulnerabilidad. Porque luego al final, después de los tiempos iniciales, de los tiempos románticos, del *hacking* original, del Homebrew Computer Club, al que se presentaban novatillos, personas como Steve Jobs o Stephen

cve: DSCG-12-CM-126

Wozniak o Bill Gates, que presentaban sus descubrimientos ante personas que ya eran consideradas auténticas autoridades en la materia, después de esos tiempos primigenios todo se ha convertido en herramientas que los especialistas llaman de botón gordo, es decir, herramientas que cualquier persona sin unos conocimientos avanzados puede manejar. Por ello, existen aplicaciones descargables a través de Internet que pueden organizar auténticos desastres en malas manos. Muchas veces son herramientas que tienen múltiples usos y que pueden servir para autoprotegerse. Por ejemplo, un *sniffer*, un analizador de tráfico en red, puede servir para saber si dentro de la red privada de mi domicilio está circulando información que no debería circular. ¿Por qué? Porque alguno de los dispositivos que maneja mi familia está infectado con algún *malware* que está exfiltrando datos y que no debería hacerlo. Un analizador de tráfico en red me puede permitir detectar ese fallo, pero ese mismo programa —por ejemplo, Wireshark, que es el más conocido— puede ser utilizado, una vez que hemos ingresado en una red insuficientemente protegida, para capturar datos particulares, datos reservados del resto de personas que están conectadas a esa red, con lo cual una herramienta que en principio es de doble uso, en virtud de la persona que lo utilice puede convertirse en una herramienta o en una arma para cometer un delito.

Les decía que estos grandes conglomerados empresariales tienen ese gran poder económico; de hecho, alguno de ellos tiene una facturación que es superior al producto interior bruto de muchos países, y el problema es que se están cansando de nosotros como Estados. Alphabet, la empresa matriz propietaria de Google, ya ha iniciado los trámites para convertirse en entidad financiera y de crédito, es decir, para tener un poder económico más allá del que dan simplemente sus ingresos a través de sus aplicaciones, que tienen un pequeño fallo, y es que se basan fundamentalmente en la publicidad. La distopía ciberpunk está más cerca con estos pasos, porque llegará un momento en el que decidan desobedecer a los Estados y estos no tengan fuerza para imponerse. ¿Por qué? No porque la ley no permita hacerlo, sino porque es el código informático el que no va a poder hacerlo. Tenemos un ejemplo perfecto en el incidente terrorista de San Bernardino el 14 de diciembre de 2015, cuando unos terroristas yihadistas radicales atacaron un centro de asistencia social —precisamente uno de los atacantes era un extrabajador de ese centro— y causaron catorce víctimas. ¿Y con qué se encontró el FBI, una de las agencias de investigación más conocida y poderosa del planeta? Con que la propia Apple le estaba diciendo: No es que yo no le quiera dar la información que usted me pide, es que la tecnología que hemos implementado para garantizar la privacidad de nuestros usuarios no nos permite darles esos datos. O sea, es el código informático, es la ley la que impide la efectividad del poder del Estado. Con lo cual, esta posibilidad de que las empresas, sobre la base del código informático, se declaren —digámoslo así— en rebeldía o se consideren señores feudales, está presente; de hecho, sin ir más lejos, la socióloga Saskia Sassen, Premio Príncipe de Asturias de 2013, nos lo advirtió en un clarificador artículo publicado el día 13 de este mismo mes en el diario *El País*, titulado *Los nuevos depredadores*, donde hablaba precisamente de esto, de estas empresas que se comportan como depredadores. Es lo que les he dicho: no existe un territorio que pueda ocupar el Estado nación.

Evidentemente, soy un servidor del Estado; como les he dicho, juré defender el Estado. Por lo tanto, esta situación no resulta agradable para mí. ¿Cuál es la respuesta que está dando el Estado ante el avance de estas fuerzas hostiles —césar, césar, los bárbaros están a las puertas de Roma—? Son dos pasos bastante preocupantes. En primer lugar, un proceso de militarización de la red y, en segundo lugar, un proceso de huida al derecho administrativo dentro de Internet. En cuanto a la militarización, han visto los términos que empleaba mi predecesor, el anterior compareciente: tigres, atacar, disparar, rifles. Basta con consultar el *Diario de Sesiones* y ver quiénes han comparecido en esta Comisión: Mando Conjunto de Ciberdefensa, Centro Nacional de Protección de Infraestructuras y Ciberseguridad, CCN-CERT. Todas son estructuras pertenecientes a escala policial o militar. En cuanto hablamos de empresas, también; son empresas de ciberseguridad. De hecho, se han celebrado en diciembre de este pasado año 2018 las XII Jornadas STIC, organizadas por el CCN-CERT, por el Centro Criptológico Nacional, y su *leitmotiv* ha sido: «Ciberseguridad, hacia una respuesta y disuasión efectiva». Respuesta y disuasión, términos clásicamente militares, de estrategia militar.

En cuanto a la huida al derecho administrativo, no hay más que ver el Real Decreto 12/2018, que ha sido aprobado prácticamente por unanimidad y traspuesto a nuestro ordenamiento jurídico el pasado 7 de septiembre. Hay una serie de autoridades, tal y como nos exigía la Directiva NIS, Network and Information Systems. Esta Directiva NIS exigía que hubiera puntos de contacto, que hubiera autoridades de notificación y, por supuesto, equipos de respuesta, pero de nuevo hago mías las palabras del anterior compareciente, busca que las estructuras sean lo más simples y unitarias posible, una autoridad

cve: DSCG-12-CM-126

competente para recibir notificaciones, y, en lugar de eso, tenemos cinco, cinco que en principio están llamadas a entenderse entre ellas y a coordinarse en un organismo superior que depende del departamento de seguridad nacional, que es el Consejo Nacional de Ciberseguridad, pero haber dado esas competencias directamente a ese Consejo Nacional de Ciberseguridad para tomar las últimas decisiones y no repartirlo entre cinco organismos hubiera sido bastante más productivo y hubiera dado lugar a un esquema mucho más simplificado. En cualquier caso, todas estas instituciones pertenecen, como ya les he dicho, al estamento policial o militar. Hay una cosa que a mí me preocupa mucho, porque me parece incluso peor todavía, hay una autoridad de notificación que ni siquiera tiene forma de derecho público, es una empresa, una empresa pública, pero es una empresa, que es el Instituto Nacional de Ciberseguridad. Su forma jurídica es la de empresa pública dependiente de la Secretaría de Estado para el Avance Digital, pero tiene forma de empresa. Que una empresa tenga autoridad, sea considerada autoridad en el concepto jurídico que tenemos del término, me resulta chocante.

El problema es que estamos hablando de ciberseguridad, incidentes de ciberseguridad, actos incluso de ciberguerra. Cuando pasa algo en materia de ciberseguridad, tenemos unos preceptos muy claros en el Código Penal, el artículo 197 bis a 197 quinquies y el artículo 264 a quáter, que están hablando de los accesos ilícitos a sistemas de la información y de los ataques y daños causados en sistemas de la información. Son delitos, tipificados penalmente, así que yo me pregunto: ¿Por qué en este real decreto, si uno hace una búsqueda en el documento PDF, no encuentra ni una sola mención a justicia, ni una sola mención a Poder Judicial, y solo una, residual, al ministerio público, a la fiscalía, diciéndole que en su caso se le notificará? ¿Por qué no está completamente integrado en este esquema de ciberseguridad, habida cuenta de que si se produce lo que no se tiene que producir, si se produce el incidente, una vez que se haya notificado y se haya resuelto, habrá que perseguir a los responsables? El problema es que este real decreto es hasta cierto punto bastante ambiguo y laxo: deja muchas cosas en el tintero. No lo digo yo, lo dice el doctor Carlos Galán Pascual, que es asesor del CCN-CERT, que es doctor en Informática y además es abogado, toca ambos palos. Concretamente, en el número 132 de la revista SIC —una revista sobre seguridad de la información—, enumeró —tuve además el placer de publicar un artículo en el mismo especial dedicado a este real decreto— las principales carencias: identificación de los factores específicos en los sectores de los operadores de servicios esenciales, determinación de las autoridades competentes, sobre todo las sectoriales. Les recuerdo que el real decreto-ley habla de que puede haber una autoridad sectorial por cada ministerio afectado y que todavía no se ha definido cuál es. En principio, en el ámbito privado, va a ser Incibe a través de la Secretaría de Estado para el Avance Digital. Dentro de las funciones de las autoridades competentes, el establecimiento de canales de comunicación, la identificación de los operadores de servicios esenciales que afecten a la defensa nacional, los supuestos de especial gravedad que requieren la coordinación nacional del CCN, la determinación de mecanismos de coordinación de los CSIRT con la Oficina de Coordinación Cibernética del CNPIC, la determinación de las medidas técnicas y de organización, la fijación de plazos para las comunicaciones a la autoridad competente, la determinación de qué sucesos o incidentes pueden afectar a las redes y sistemas de información o cuáles son las medidas necesarias relativas a la notificación de incidentes.

Les voy a decir una cosa: en principio el reglamento todavía no se ha publicado, y la verdad es que, viendo otras normas capitales como puede ser la Ley del juego, aprobada en 2011 y cuyo reglamento se demora en el tiempo, quiero ser optimista, pero tengo miedo, tengo el legítimo temor de que este reglamento se demore demasiado en el tiempo, porque entretanto determinadas instituciones, como el CCN, el CNPIC o Incibe, hacen circular una guía nacional de notificación de incidentes de ciberseguridad, que se está haciendo circular a aquellas personas encargadas de la seguridad informática, por ejemplo, en grandes empresas, como compañías eléctricas. Los CISO, Chief information security officer, son los que están refiriendo estas guías, cada una con su correspondiente marca de agua, con lo cual no les puedo decir eso de que he tenido acceso a una de estas guías, no porque sea un documento secreto sino porque estaría delatando a la persona que me lo facilitó, que es el CISO de una gran empresa. Todas estas carencias que les he ido enumerando, que van a tener que formar parte del reglamento, ya están previstas en esta guía, ya automáticamente estas instituciones policiales, militares y empresas se están irrogando estas facultades normativas en una pseudo norma que no es tal norma. Es decir, están publicando una guía que en la práctica está actuando como un reglamento y no lo es, porque estas instituciones no tienen esta competencia reglamentaria. Así pues, si bastante grave es que no se hayan especificado estas cuestiones en un texto legal que emane de las Cortes Generales —y hemos tenido que acudir a una delegación reglamentaria comprensible siempre que hablamos de materias alta complejidad

cve: DSCG-12-CM-126

técnica—, mucho más grave todavía es que tengamos una mera guía de buenas prácticas que está señalando plazos concretos en los que hay que notificar determinados incidentes. Se supone que estas autoridades van a poder proponer, y yo entiendo que proponer únicamente y que no van a ser capaces de implantar ellos mismos las sanciones, porque entonces ya sería el acabose. Volviendo a una metáfora con el mundo físico, como hizo el anterior compareciente, sería como si el guardia de tráfico o el vigilante de la zona azul no solo tuviera en un folleto que él mismo ha elaborado la normativa que deben seguir los conductores, sino que sus meras denuncias actuasen como multas. Recordemos, si la Guardia Civil les para en carretera y extiende un boletín, es un boletín de denuncia, no les han puesto una multa, pese a que el idioma coloquial nos diga lo contrario; han formulado una multa que cuando se resuelva el expediente administrativo sancionador, dará lugar a una sanción en forma de multa. Estamos confundiendo el resultado final con el acto iniciador. Bien, quiero pensar que estas instituciones no se están irrogando la facultad de imponer ellos mismos las sanciones, porque entonces sería el apaga el Estado de derecho y vámonos. Quiero pensar que este reglamento va a recoger como meras sugerencias lo que están diciendo estas guías de notificación de ciberincidentes, pero francamente, me preocupa, me preocupa que el tercer poder del Estado, la justicia, sobre todo la fiscalía, que digamos es el brazo llamado a promover la acción de la legalidad en defensa de todos los ciudadanos, no esté invitado a esta fiesta. Por lo tanto, como les digo, esta guía nacional adopta una vestimenta formal de mera guía de recomendaciones, pero en el fondo está actuando como una norma; de hecho, los CISO dicen ¿pero esto qué es? No es un reglamento y nos están diciendo los plazos en los que tenemos que notificar el tipo de incidencias, cuáles son las graves, las menos graves, las críticas, que es otro término que también tiene mucha enjundia, señorías.

La Directiva NIS hablaba de servicios esenciales y no esenciales, punto. Pero aquí tenemos una Ley de protección de infraestructuras críticas, y entonces para no generar antinóminas en nuestra legislación, hemos dicho: ¿equiparamos las infraestructuras críticas con las esenciales? No. Hay unas que consideramos críticas y otras que consideramos esenciales. ¿Se puede ser crítico sin ser esencial? No. ¿Se puede ser esencial sin ser crítico? Sí. Pues que alguien me lo explique, de verdad; me gustaría que alguien me explicase cómo una actividad puede ser esencial y no ser crítica, porque yo creo que es lo mismo, simplemente le hemos puesto distinto nombre porque era una norma de rango europeo que venía en unos idiomas oficiales que no son el nuestro y hemos sufrido un *lost in traslation*, nos hemos perdido en la traducción. Así pues, entiendo que se ha duplicado el número de trámites que tenemos que seguir para notificar un incidente añadiendo esta distinción entre crítico y esencial.

De la misma manera, también tenemos una Ley de la Función Pública, con lo cual se distingue entre aquellos órganos de notificación, aquellas autoridades a efectos de notificación que se ocupan del sector público y aquellas que se ocupan del sector privado, y ahora es cuando lo mezclamos todo en la coctelera y servimos un Martini con vodka, agitado o batido, según la preferencia del James Bond de turno. Es decir, ¿institución pública esencial o no esencial?, ¿crítica o no crítica?, ¿privada, pública o no pública? ¿Afecta a la defensa nacional? Por ejemplo, unos astilleros forman empresa pública, es decir, en principio gira en el tráfico jurídico como una empresa, pero en la práctica pertenece al Estado. ¿Es público o privado? ¿Es un servicio esencial? Bueno, si les preguntan a los habitantes de Cádiz si Navantia es un servicio esencial, les contestarán con todo su buen sentido que, por supuesto, que sin Navantia Cádiz tendría un problema de paro muchísimo más grave que el actual. ¿Afecta a la defensa nacional? Bueno, en estos momentos está construyendo unos buques de acción marítima que tienen una serie de armas auténticamente imponentes, unos cañones capaces de destrozarlo todo a su paso. Esto parece que afecta a la defensa nacional, sin embargo, se los vamos a vender a un tercer país, con lo cual, en principio, no están afectando a nuestra propia defensa nacional. El problema es que, según eso, vamos a tener que ir cambiando de ventanilla. Esto al final puede acabar pereciendo la única de las doce pruebas de Asterix y Obelix, que están a punto de fracasar, que es enfrentarse a la burocracia. Imagínense las doce pruebas de Hércules, el león de Nemea, la hidra, todas esas pruebas son *peccata minuta* para los dos héroes galos, pero cuando se topan con la burocracia francesa, gala, en el supuesto de la ficción, están a punto de tirar la toalla; pues, imagínense a expertos en seguridad informática que tienen que toparse con nuestra burocracia. ¿Esto es crítico o no es crítico? ¿Es esencial o no es esencial? A ver, consulta el cuadro.

En esos momentos lo que importa a los informáticos de una compañía, de una empresa o de una institución, los que están en el SOC, es mitigar esa incidencia, es parar su resultado. Te ataca el WannaCry, todos tus ordenadores ven sus datos bloqueados. ¿Eres una compañía como Movistar Telefónica? Tienes un problema. ¿Eres una red de hospitales como la que se vio afectada en Gran Bretaña? Tienes un problemón. Y si sobre todo en lo que llaman ahora amenazas híbridas, alguna mente perversa se decide

cve: DSCG-12-CM-126

a combinar ese ataque del *malware* WannaCry con lo que sucedió apenas dos semanas después: nada más y nada menos que un lobo solitario yihadista que decide inmolarse haciendo detonar un chaleco explosivo a la salida de un concierto de una estrella juvenil, Ariana Grande, provocando dieciséis muertos y varios centenares de heridos, imagínense que esas dos actuaciones se coordinan y en el momento en el que explota la bomba y hay que empezar a evacuar heridos, de repente todos los hospitales tienen sus datos cifrados. Por supuesto, nos dirán que lo más importante es que las máquinas de TAC, las máquinas de resonancia magnética nuclear están separadas. Muy bien, fantástico. Llegan centenares de heridos —mi hermana, que es médico de urgencias, me tiene dicho que en un hospital del tamaño de una ciudad sanitaria como la Juan Canalejo, de A Coruña, basta con cinco o seis heridos en una situación crítica para colapsar un servicio de urgencias—, imagínense, se tendrían que repartir por todo el área metropolitana. Lo primero que hay es la atención básica, el triaje sanitario. ¿Necesita una transfusión? Sí, la necesita porque ha perdido mucha sangre. Vamos a hacer la transfusión. No podemos, no sabemos su grupo sanguíneo. Consulta el historial. No se puede, está cifrado. ¿Por qué? Por el WannaCry. Vamos a inyectarle algún tipo de medicación, adrenalina, lo que sea. No podemos. ¿Por qué? Porque no sabemos si es alérgico, su historial clínico está cifrado. Es decir, las máquinas más importantes, la resonancia magnética nuclear, pueden estar protegidas, pero resulta que lo más básico, que es el historial clínico de los pacientes, no está protegido y ha sido cifrado por un *malware*.

Como les digo, la existencia de estas amenazas híbridas es una auténtica pesadilla para los expertos en ciberseguridad, pero también para los expertos en ciberdelincuencia, porque ¿cómo vamos a perseguir este incidente si sucede? Porque si sucede ya no es incidente de ciberseguridad o un acto de ciberguerra. La guerra, tal y como me enseñaron a mí, es cuando un Estado ataca a otro; cuando se trata de un ataque a un país, a sus infraestructuras o a sus ciudadanos por parte de un particular, de una banda criminal o de un grupo del que no sabemos su filiación, hay un acto de delincuencia, y ese acto de delincuencia tendrá que ser reprimido, si es posible por las Fuerzas y Cuerpos de Seguridad y posteriormente tendrá que ser perseguido por la justicia. ¿Cuántos procesados hay en este momento en España por el incidente de WannaCry? Que yo sepa, ninguno. La policía no tiene medios suficientes ni dispone de las capacidades suficientes para haber llegado a determinar quién es el autor de la infección de este *malware*, quien lo desarrolló, quien lo implantó en los sistemas informáticos de empresas españolas. Vivimos en la absoluta impunidad de estos grandes delitos. Evidentemente, como fiscal especializado en ciberdelincuencia, me veo con otro tipo de ciberdelincuentes, como pueden comprender. No es el objeto de esta Comisión, aunque parezca serlo, porque si se leen, insisto, esta guía nacional de notificación de incidentes, algunos de los incidentes que consideran de baja peligrosidad es que se difunda *spam*, que haya tránsito de pornografía infantil por los sistemas informáticos de una empresa o institución pública, que haya estafas a través de *phishing*, que se esté reconduciendo a los navegadores de Internet a sitios fraudulentos para robo de información. Eso lo consideran incidentes de ciberseguridad, son delitos tipificados en el Código Penal, es decir, son el grueso de la memoria de la Fiscalía General del Estado en materia de ciberdelincuencia; además de estos incidentes de ciberseguridad de alto nivel en los que ya les digo que carecemos de la capacidad técnica suficiente para llegar a imputar a los autores de los mismos. Pero es que ya se están metiendo incluso en los delitos más básicos de nuestro día a día considerándolos como incidentes de ciberseguridad y diciendo que dado que su grado de impacto es bajo, la notificación es voluntaria. Bueno, la notificación será voluntaria a estas instituciones de ciberseguridad, pero les recuerdo que existe la Ley de Enjuiciamiento Criminal que dispone la obligación de denunciar los delitos. El problema es que las multas son de 125 pesetas porque tenemos una Ley de Enjuiciamiento Criminal de 1882. Hay que tener en cuenta el grado de impacto, la gravedad de la amenaza, por ejemplo, lo que llamamos un escaño de puertos, que también se ha mencionado por el anterior compareciente. Como saben, la información no circula por los cables de uno en uno, porque si no, se atropellarían. Se asignan puertos lógicos, que son distintos carriles por los que circula cada información. Si voy a consultar una página web, mi navegador utiliza el puerto 8080; si voy a mandar un correo electrónico, mi programa de correo electrónico utiliza el puerto 295. Esos son los puertos. Un escaneador de puertos, como puede ser la aplicación Nmap —que se puede descargar gratuitamente de Internet— permite lanzar una tentativa de ataque diciendo: a ver qué puertos tiene abiertos un determinado sistema informático, que puede ser el ordenador de mi casa, el *router* de mi casa o puede ser la infraestructura de una compañía de producción de energía eléctrica. Sin ir más lejos, una compañía de tamaño medio como pueda ser Endesa, Viesgo o Fenosa pueden tener una media de 675000 escaneos de puertos diarios. El otro día, hablando con un CISO me dijo que habían tenido un día bastante agitado y que habían tenido un pico de 2 millones de

cve: DSCG-12-CM-126

escaneos de puertos. Evidentemente, el atasco que sufren los juzgados dedicados a las cláusulas suelo palidecería en comparación con cualquier juzgado de instrucción que recibiera notificación de estos 675000 escaneos de puertos como tentativa de un delito de acceso ilícito a sistemas informáticos, porque lo que se está utilizando es una herramienta que está prevista en el artículo 197 ter, apta para cometer este delito. Es decir, en principio deberíamos perseguirlo, pero claro, 2 millones de delitos en un día me temo que no hay Administración de Justicia que lo soporte.

Los CISO están preocupados no solo por estos intentos, sino por las tentativas que al final acaban consumándose, las exfiltraciones de datos. Hace poco consulté el informe de ElevenPaths, la unidad de ciberseguridad de Telefónica, del último semestre de 2018 y decían que, en respuesta a ciberincidentes causados por *malware*, la media de respuesta era de tres días/tres días y medio. Eso son eras geológicas en términos informáticos. Las más rápidas eran las compañías de seguros, que tardaban una media de dos días; las compañías de alimentación podrían tardar cuatro días; las empresas de entretenimiento podrían tardar diez días en resolver un incidente. Y esto una vez detectado, porque ese *malware* puede haber estado residiendo en su sistema durante meses o años. En cuanto a vulnerabilidades, nuestro Código Penal define el delito del 197 bis como el que cualquier medio o procedimiento, sin estar legítimamente autorizado y vulnerando medidas de seguridad, tenga este acceso no permitido. Bien, ¿qué pasa cuando la medida de seguridad tiene una vulnerabilidad o cuando directamente no hay tal medida de seguridad? El caso se ha dado aquí mismo: despacho de abogados en el Paseo de la Castellana que tiene datos de sus clientes almacenados en un servidor FTP de protocolo de transferencia de archivos. No tiene autentificación, nadie le pide un usuario ni una contraseña cuando se accede al mismo. ¿Qué pasa? Que un día un chaval está utilizando Shodan —un buscador como Google, solo que se dedica a buscar aplicaciones, procesos; no busca páginas web— y le dice que ese servidor FTP está abierto, sin autentificación, y mira a ver qué hay y empieza a descargar archivos y archivos. La Policía Nacional entra en funcionamiento porque es el servidor de un despacho de abogados y se ha vulnerado el secreto profesional entre abogado y cliente, y es más, desde el primer momento se ha cometido un delito contra la intimidad porque se están descargando expedientes confidenciales. Pero, en principio, no hay delito de acceso ilícito como tal porque el sistema no tenía ninguna medida de seguridad.

Otro tanto pasa con las vulnerabilidades. En teléfonos móviles con sistema operativo IOS en el último semestre del año 2018 esta compañía detectó cerca de 165 vulnerabilidades corregidas; corregidas, imagínense las que todavía no se han detectado. Otro tanto hay en los sistemas Android o más. Son vulnerabilidades que pueden permitir la ejecución remota de códigos, es decir, que alguien tome el control de su máquina, que alguien tome el control de su ordenador, de su teléfono móvil, de su frigorífico. Sí, de estas neveras que aparecen en la publicidad con conexiones a Internet. Porque es que tenemos muchos aparatos conectados como por ejemplo la nevera. ¿Cómo que la nevera? Sí, la nevera porque te avisa de si los yogures están caducados para pedir más al supermercado. Bien, hay dispositivos en lo que llamamos el Internet de las cosas, como frigoríficos, cafeteras que son vulnerables. La última vez que fui a comprar cápsulas de una conocida marca de cafeteras, me encontré con que ya había un modelo de cafetera que se conectaba a la red *wifi* para que se pudiese cargar el *ristretto* desde tu casa, mientras ibas en el autobús. Bien, ¿y esa cafetera tiene antivirus? No. ¿Tiene *firewall*? No. ¿Se conecta a través de una VPN? No. ¿Y para qué necesita todas esas cosas una cafetera? Muy sencillo porque en el ataque del *malware* Mirai que echó abajo la infraestructura de la mayor compañía de resolución de direcciones DNS, o sea, la que convierte los números de las direcciones IP en direcciones que podamos teclear —por ejemplo, www.google.es— una de las mayores compañías de todo el mundo, que se llama DynDNS, que tiene su sede en la costa oeste de Estados Unidos, sufrió un ataque con el *malware* Mirai que provocó que cerca de doce horas todos sus clientes no tuvieran conectividad a Internet. ¿Qué clientes? Twitter, el *Wall Street Journal*, Amazon, Ebay. Todo esto desapareció de Internet porque no había posibilidad de teclear estas direcciones de Internet y que alguien resolviera esos nombres de dominio y los transformara en direcciones IP. ¿Y qué tiene de particular este virus Mirai? Que la mitad de los dispositivos infectados eran aparatos de Internet de las cosas, sobre todo cámaras de videovigilancia, cámaras IP que nadie nunca había configurado para que tuvieran un usuario y una contraseña.

En el futuro serán dispositivos *wearable*, es decir los relojes que llevamos para salir a hacer *running* —o sea correr de toda la vida—, cafeteras, neveras, termostatos; todos esos dispositivos que básicamente tienen un pequeño ordenador dentro y que son susceptibles de ataques de negación de servicio, por lo cual pueden afectar a infraestructuras críticas. Ya les he mencionado un simple ejemplo como es el de un hospital. Imagínense una central nuclear, una central eléctrica o, por supuesto, pequeñas y medianas

cve: DSCG-12-CM-126

empresas. Cuando arreció el primero de los grandes *ransomwares*, que utilizaba una vulnerabilidad en Windows Exchange Server, versión de 2003, la mayoría de los afectados eran pequeñas y medianas empresas: talleres, gabinetes odontológicos, despachos de abogados, que llegaban con unas denuncias, con unos atestados que ponían los pelos de punta. Decían que iban a tener que cerrar, que toda su documentación estaba cifra y no había ninguna posibilidad de recuperarla. Pues bien, resulta que hay expertos en seguridad informática que poco a poco han ido dando con las soluciones a estos problemas, gente que participa en estas convenciones de *hackers* y que expone estos descubrimientos. Gente como Yago Jesús, un experto en seguridad informática, que es probablemente la mayor autoridad en materia de *ransomware* en España y el primero en crear una vacuna contra un determinado tipo de *ransomware* para evitar que los ordenadores puedan ser cifrados a través de este tipo de programas. Estas personas, en principio, quieren colaborar, lo que no encuentran es cómo, porque nuestro artículo 197 bis no establece ningún tipo de protocolo de comunicaciones o de salvaguarda de estas personas. Así que si alguien obtiene un acceso no autorizado a un sistema y lo notifica, ya puede hacerlo a través de un abogado para que le tutele el secreto abogado-cliente o directamente se puede enfrentar a una denuncia del afectado porque aquí seguimos la máxima de matar al mensajero: antes de que piensen que mis sistemas informáticos son vulnerables lo que voy a hacer es decir que este señor es un *hacker* muy malvado. Ha pasado con cuestiones auténticamente ridículas. Hace ya varias legislaturas el Centro de Investigaciones Sociológicas sufrió una filtración de su baremo sociológico, de la oleada correspondiente a un trimestre de 2010 o 2012, no recuerdo exactamente. El responsable era un sociólogo que tenía bastantes conocimientos informáticos y se dio cuenta de que todos los barremos, los archivos PDF donde estaba el barómetro sociológico, se encontraban en direcciones de Internet que terminaban en un número correlativo —3, 4, 5…—; así que simplemente buscó la que todavía no estaba publicada, puso un 6 y, ¡bingo!, ya estaba colgada, solo que no tenía ninguna medida de seguridad.

¿Qué hizo el Centro de Investigaciones Sociológicas? Pues decir: Nos han *hackeado*. Si poner un número correlativo es *hackear*, es decir, si el último número del que tengo conocimiento acaba en seis, y añado a la dirección un siete, si eso es *hackear*, señorías, entonces mi hija de once años es *hacker*, porque hasta ahí llega. Estas personas tienen miedo a colaborar —antes hablábamos de colaboración público-privada—, tienen miedo a verse investigadas y están muy preocupadas con redacciones legales como la que tiene el Código Penal actual. Evidentemente, modificarlo a estas alturas es difícil porque requiere unos consensos legislativos que son complicados de alcanzar, sí, pero si a través de este instrumento, de este Real Decreto 12/2018, hubiéramos establecido una mayor participación de la fiscalía estableciéndolo como canal seguro de notificaciones de particulares que tuvieran un interés no espurio, que no quisieran aprovecharse de estos datos, de estas vulnerabilidades, sino que quisieran notificarlas, que quisieran ayudar al Estado o a las empresas privadas, la fiscalía podría protegerles, podría protegerles como denunciantes de una vulnerabilidad. Voy más allá aún: si la fiscalía tuviera conocimiento de una vulnerabilidad y notificara la existencia de la misma a la institución afectada, esta persona se convertiría automáticamente en garante, tendría la posición de garante y estaría obligada a modificar estos sistemas informáticos para que esta vulnerabilidad fuera corregida. Si no lo hace, según el artículo 11 del Código Penal, responde de los daños que puedan surgir por su culpa por terceras personas, por omisión, por no haber hecho lo que se le pedía. Así pues, el artículo 197 bis, ter, quater y quinquis, y el 264 hasta el quater contemplan que estos delitos puedan ser cometidos por personas jurídicas, con lo cual, si la fiscalía tuviera esta potestad de requerir a estas entidades para que solucionen sus agujeros de seguridad podría convertirles en responsables hipotéticos de un delito cometido en comisión por omisión, con lo cual no estaríamos hablando de multas, estaríamos hablando de la última ratio del Estado, el Código Penal, la última herramienta para protegernos de las conductas más intolerables. **(El señor presidente ocupa la Presidencia).**

Entiendo que la responsabilidad que tienen estas grandes empresas que tutelan de forma vicaria unos datos que no les pertenecen, que no son suyos, que son de los ciudadanos o que pueden afectar a los ciudadanos, tendría que estar en los tribunales de justicia y por eso la fiscalía debería haber tenido una mayor implicación en esta herramienta de ciberseguridad tan fantástica como es el real decreto de trasposición de la directiva comunitaria sobre medidas para dotar de seguridad a los sistemas y redes de información, y es por ello por lo que en fase de desarrollo legislativo reglamentario imploro a sus señorías —como diría el personaje de la película *Jerry Maguire*—: ayúdenme a ayudarles. Ayúdenme, ayúdennos a que estas herramientas puedan ser útiles, puedan ser ágiles; inclúyannos, sobre todo a la red de fiscales especializados en ciberdelincuencia. Yo soy uno de ellos, uno más, igual hago más ruido que el resto y

cve: DSCG-12-CM-126

por eso se han fijado en mí, pero les aseguro que hay excelentes profesionales con un nivel de conocimiento asombroso y esas personas están esperando poder colaborar con ustedes para solucionar la gran amenaza, no del futuro, como todo el mundo me decía cuando les dije que mi especialidad era la ciberdelincuencia, no, sino del presente; la gran amenaza del presente que es la ciberseguridad cuando falla y se transforma en ciberdelincuencia.

Nada más y muchas gracias por su atención, señorías. Espero no haberme excedido del plazo de tiempo.

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

No puedo testificar si se ha excedido o no porque he tenido que estar fuera, pero por la cara de sus señorías me parece que ha estado usted muy bien. Vamos a ver si continuamos con este alto tono y le podemos ayudar en el tema.

Ahora tiene la palabra el señor Salvador.

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

En primer lugar quiero manifestarle que las comparecencias que hemos tenido esta mañana me han hecho recordar los inicios del desarrollo de la sociedad de la información en nuestro país, pero muchos años después —estamos hablando ya de prácticamente trece años desde el Plan Avanza y antes con los elementos que se intentaban poner en marcha desde la Administración—, y me estoy retrotrayendo hasta esa época porque buena parte de las intervenciones, por lo menos del primer ponente e incluso de usted mismo, tienen que ver con ese origen y con algo que voy a decir ahora, con problemas no resueltos todavía después de tantos años y de un desarrollo que en su momento no los abarcaba. Por ejemplo, nos planteábamos quiénes estaban en Internet y entonces estaban los ciudadanos que querían ver de qué iba eso, pero no estaban las empresas, ni las administraciones, ni el negocio. Muchas veces he dicho que, ante el *total free* de Internet de compartirlo todo gratis, después los periódicos entraron a decir que la información que se compartía y que estaba transmitiéndose tenían que cobrarla porque, si no, si no tenían papel, tenían que cerrar. Todo ese modelo de negocio, que es el que ha costado tanto trabajo y que está dando tantos problemas, tiene mucho que ver con ese Internet de ese momento del *total free* libre, beta. Conozco a Francisco Hernández, un fiscal también especializado y con el que he compartido muchos momentos de conversación vinculados a estos temas, y es verdad que usted viene aquí a aportarnos soluciones desde su visión y, al mismo tiempo, al final nos ha pedido socorro y ha detectado que hay un problema de gobernanza del propio desarrollo de la ciberseguridad. Al final, ese reglamento que usted ha dicho debiera desarrollarse y establecer cuál es el papel de cada cual, también desde el concepto de la división de poderes, que se puede vulnerar. Al final son otras empresas las que actúan porque se han anticipado o porque son las primeras respuestas que se han puesto en marcha para poder contener el ciberdelito, etcétera. Esos organismos que usted ha dicho que están funcionando bien y están prestando una gran labor y un gran servicio, pero al mismo tiempo es verdad que probablemente cada cual tiene que ir encontrando su espacio y es muy importante que la justicia encuentre el suyo.

Respecto a esto que nos dice usted de ayúdenme a ayudarles, que yo he compartido siempre —lo digo porque lo he detectado personalmente—, en la propia justicia las cosas también dependen de la mentalidad de la persona que coja un tema y de cómo lo analice. Por poner un ejemplo, que ya he expuesto alguna vez en esta Comisión, cuando hubo un bulo muy importante y muy dañino que circuló sobre mi persona haciéndoselo llegar a los partidos políticos, yo seguí el cauce reglamentario: cogí los correos que me había mandado algún compañero y me fui a la policía; la policía fue al juez; el juez dijo que, como era una cosa de políticos porque me lo había pasado un político, lo mandaba a Madrid desde Granada. Yo pedía la dirección IP para saber la persona que podía haberlo hecho —teníamos cierta sensación de quién podía ser— y actuar. Después lo archivaron porque decían que no había habido denuncia. ¿Cómo va a haber denuncia si no sabemos de quién es y la policía hace su trámite también, tiene que ir a la justicia y la justicia no le da la respuesta? Es decir, el sistema es el que está funcionando mal y eso está permitiendo que a río revuelto ganancia de pescadores. Entonces, comparto completamente su visión y comprendo que todavía hace falta una adaptación del conjunto de la sociedad y entender que lo digital tiene que ver también con lo analógico y que estamos hablando de una extensión y de un ámbito más que es abierto. Antes nos hablaban de los cuatro ejércitos y usted se ha referido también a la dimensión espacial, pero ciñéndonos a esto es verdad que lo digital es un ámbito más, que es como los demás, pero que no está contemplado ni recogido de la misma manera.

cve: DSCG-12-CM-126

Quisiera preguntarle: en la parte que nos toca a nosotros, en el cambio de legislación y en propuestas, ¿qué podemos hacer para que la justicia ocupe el lugar de gobernanza que se requiere en este ámbito y que no sea algo del reparto del día a día, de cómo vamos actuando poniendo medidas o cómo vamos poniendo parches para tapar vulnerabilidades y huecos? Hay que ver cuál es el papel de cada cual: cuál es el papel de la Administración, cuál es la colaboración público-privada, cuál es el papel de las Fuerzas y Cuerpos de Seguridad del Estado, cuál es el papel de la justicia y cómo dotamos de esa gobernanza al sistema y, sobre todo, cómo protegemos a los ciudadanos que son los que lo soportan. El compareciente anterior hablaba de las pymes, de cómo se ven afectadas, de los problemas que tienen y que nada está diseñado tampoco para protegerlos a ellos o del usuario final con el que también sucede lo mismo, por ejemplo, con el supuesto que le he puesto antes. Entonces, hacen falta medidas para poner en orden esta gobernanza. En qué podemos ayudarles también para que no sea simplemente la interpretación de un juez que esté formado en este tipo de temas y especializado, sino que cualquier juez sepa que hay ciertas cosas que tiene que hacer y que amparan los derechos de un ciudadano y que no depende de quién se lo coja para que le atiendan bien o se vea desprotegido; en qué podemos ayudar.

Muchas gracias.

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

Señora Angustia.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Buenas tardes ya, señor Bermúdez; muchas gracias por venir. Cada vez que termina una sesión de esta Comisión me voy a mi despacho, luego a mi casa y el fin de semana a casa de mi abuela y reviso todas las posibles vulnerabilidades que pueda tener; es un sinvivir y así cada sesión. **(Risas).**

Hay una constante a lo largo de toda su intervención que es no solo la falta de consultas sino la falta de presencia de los operadores jurídicos a lo largo de muchos desarrollos. Muchas veces hemos intentado en estas sesiones resaltar esto, y la última vez, además, era coincidente con algo que señalaba yo misma hace como un par de sesiones y justamente con el mismo artículo de referencia que parece que ambos hemos leído— que es la ausencia total, como agentes activos, que tienen los operadores jurídicos en el real decreto. Por eso, le agradezco que aceptase la invitación que, a través de la Mesa de esta Comisión, le hizo mi grupo parlamentario, para poder aportar todas estas cuestiones sobre las que, si ha seguido las ponencias, y yo creo que sí, todavía estamos un poquito verdes no solo de desarrollo sino respecto de las conclusiones. Por eso, le agradezco que estuviese.

Hay algo que, casi sin que se lo pidiésemos, los dos ponentes anteriores de esta mañana han hecho, y es pronunciarse sobre las necesidades que creen que existe sobre la formación en materia de ciberseguridad y de gestión de la información que tenemos ahora mismo; de formación reglada o de formación no reglada; no es mi intención condicionar la respuesta en este sentido, sino conocer su opinión al respecto de la formación.

Voy a ser temeraria. El sistema jurídico, evidentemente, debería adaptarse a velocidad de las TIC; siempre, evidentemente, se tipificará después. Pero no solo supone eso; hay quien cree que lo estamos haciendo bien, pero yo voy a ser temeraria y voy a decir que no, para aventurar una posibilidad de por qué a veces llegamos tarde a las cosas. Y es que puede que a veces analicemos las cosas desde el punto de vista de las tipologías, de los delitos y de las regulaciones, pero no lo hagamos desde el punto de vista de la modernización y de la tecnificación del sistema. Puede que por eso la Administración de Justicia y los operadores jurídicos, a veces, parezca que vayan un poco más por detrás de lo que sería recomendable respecto de las necesidades que el sistema jurídico tiene en materia de protección, de TIC, de ciberseguridad, de gestión de la información, etcétera. Digo que soy temeraria, pero igual no debería de serlo y sí se están contemplando todas estas cuestiones pero no nos lo parece.

También deberíamos hacer un esfuerzo mayor con respecto a la formación, tanto desde la Administración de Justicia como desde los operadores jurídicos, dentro de esa cadena de nuevas necesidades que nos genera el mundo ciber. Desde un punto de vista jurídico, también una de las cosas que posiblemente se traslade más, y no solo nosotros podríamos poner ejemplos personales, sino que es una de las inseguridades que más se traslada a nivel ciudadano, es cómo afecta a los delitos sobre el respeto a la intimidad y qué medidas estamos poniendo para solucionarlos.

Termino al hilo de algo que si no son ya nuevos delitos sí son nuevas formas consolidadas con la posibilidad de comisión de delito en el mundo virtual. Una de ellas es el Internet de las cosas, cómo avanzamos para proteger el Internet de las cosas, que ha venido para quedarse, y que también se ha

cve: DSCG-12-CM-126

mencionado a lo largo de toda esta mañana; cómo se puede mejorar para garantizar, a través de nuestro sistema legislativo, la protección de los usuarios en el Internet de las cosas. Y, por último, las criptomonedas que, evidentemente, también tienen una vinculación legislativa y jurídica esencial, porque —como decía— la posibilidad de comisión de delitos también se abre ahí, y el blanqueo y el terrorismo están íntimamente ligados a la regulación, al funcionamiento y a la aceptación, aunque ya creo que muy pocos espacios, por lo menos con poder de decisión, cuestionan que las criptomonedas están ahí, que las divisas digitales han venido para quedarse; no sé si como una herramienta financiera de futuro, no sé si se va a quedar en un complemento que parece lo que son ahora; no sé quién va a ganar el debate entre *trading* y criptomoneda y compras, pero tenemos retos jurídicos también al respecto de esto. Precisamente porque se abre un marco de necesidades de protección jurídica contra la comisión de delitos en las criptomonedas, sí me gustaría conocer su opinión.

Nada más y muchas gracias.

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

Señor Hernando.

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

Gracias, señor Bermúdez, por su presencia y por la intervención que ha hecho. Es importante para nosotros la aportación que ha hecho para poder enriquecer y mejorar las conclusiones de esta Comisión y, sobre todo, las sugerencias más concretas que nos puede hacer en materia legislativa. Al principio de su intervención usted ha dicho: Es un honor para mí estar en esta Comisión por la capacidad que tiene la misma y el Congreso de los Diputados de modificar la legislación, ya que uno de los principios fundantes del Parlamento es la capacidad legislativa. Es usted muy optimista respecto a la capacidad de esta Comisión, pero en todo caso nosotros le agradecemos que tenga ese optimismo y confianza en nuestra capacidad de modificar y mejorar la legislación en esta materia.

Le he visto crítico respecto a cómo se ha traspuesto la Directiva NIS y al Real Decreto 12/2018 y quizá podríamos empezar por ahí. Conste que no hicimos caso en su momento a algunas de las recomendaciones que nos hizo aquí una persona, a la que usted ha mencionado, que compareció en esta Comisión, que es la fiscal Elvira Tejada. Nos hizo algunas recomendaciones que convendría repasar respecto a cómo se tenía que trasponer la directiva NIS, precisamente respecto al tema de las notificaciones, que me da la impresión de que no atendimos, entre otras cosas, porque esta Comisión tenía una capacidad limitada para tal fin, pero que tampoco se han atendido en general. En este sentido y más concretamente, ¿qué tendría que hacer el reglamento que ha quedado como una laguna en la trasposición de la directiva? ¿Cuáles tendrían que ser los elementos que esta Comisión recomendase al Gobierno a la hora de ese desarrollo reglamentario, que esperemos que sea temprano? En concreto, nos ponía ahora algún ejemplo de reglamentos que están pendientes desde hace cinco, seis, siete, ocho y hasta diez años. Por ejemplo, la Ley de Asilo, que es una ley de la que yo fui ponente en su momento, es de 2010 y tiene un reglamento pendiente desde hace nueve años. Además, en este caso sería mucho más grave, porque en este tema las cosas sí que van mucho más rápido y, por lo tanto, habría que urgir a que hubiese un reglamento rápido, pero, además, que ese reglamento cubriese, en la medida de lo posible, algunas de las lagunas que es evidente que ha dejado el Real Decreto 12/2018, con el que yo creo que usted ha sido razonablemente crítico. No criticó que haya sido crítico con él sino que lo haya dicho con tantísima claridad.

¿Qué opinión le merece la nueva Ley de protección de datos personales y garantía de los derechos digitales? No sé si en su momento compareció en la Comisión que estuvo estudiando este tema. Hubo muchos comparecientes y fue una Comisión que tuvo audiencias interesantes. Esta ley es muy importante; el problema es que ha entrado en vigor hace un mes y quince días, creo. Esto es del 5 de diciembre, y debió ser publicado en el BOE del día 16 o así. Por lo tanto, tenemos muy poca capacidad de ver en perspectiva qué es lo que va a pasar con la Ley de protección de datos personales y garantía de los derechos digitales, pero quizá tenga usted alguna opinión que nos pueda venir bien de cara al futuro.

Lo que usted ha puesto de manifiesto es que el Estado de derecho tiene muchas dificultades para abordar una cosa que hasta ahora podía abordar con mucha más facilidad. Lo dice en un artículo que he visto en este libro colectivo coordinado por el fiscal Zaragoza. Es mucho más fácil patrullar las calles de Madrid que patrullar las calles de Internet, que además suelen ser particulares y conectan también centros particulares, privados, no públicos. Esta es la dificultad que tenemos. En todo caso, por ser optimista, y por eso me dedico un poco a la política, el Estado de derecho ha tardado mucho en triunfar en los 194 países de Naciones Unidas, mucho, mucho, muchos siglos. Es cierto que ahora mismo vamos por detrás

cve: DSCG-12-CM-126

de la tecnología y que, además, es mucho más difícil patrullar estas calles que patrullar las de Madrid, y tenemos que tener muchos más conocimientos tecnológicos; pero no desesperemos. Usted dice: A mí me da miedo; tengo temor a veces cuando conozco lo que hay ahí. Bueno, está bien que nos situemos desde esa perspectiva, porque eso nos obliga también al legislador, al regulador, a ponernos las pilas y hacer cosas mucho más rápidamente.

Le quería decir otra cosa. En materia de legislación penal concreta tenemos la reforma del Código Penal 1/2015, de 30 de marzo, artículo 197 —ha sido crítico respecto a este tema—, cómo habría que modificarlo para que se pudiesen lograr esas ayudas, esas colaboraciones, que permitan que todo ese conocimiento ayude al legislador, ayude a la justicia y ayude al Estado de derecho a atajar determinados comportamientos que repugnan al Estado de derecho y a la justicia. Hay un capítulo de este libro, que es precisamente el que usted escribe, *Investigación tecnológica y derechos fundamentale*s, comentarios a la reforma de la Ley 13/2015, de Enjuiciamiento Criminal, en el que usted habla del deber de colaboración de los particulares. ¿Cuál es su experiencia en este tema? Pero no de los particulares ciudadanos de a pie sino de los Gafam, de estos de los que usted ha hablado. ¿Qué experiencia tiene? Ha contado aquí una anécdota pero quiero saber qué experiencia tiene la justicia española, qué experiencia tiene usted como fiscal, si es que ha llevado algún caso relacionado con estos grandes grupos, con estos grandes proveedores, estas grandes multinacionales que se dedican a este tema.

Por último, le pregunto: ¿Cree que la fiscalía cuenta con medios suficientes para este tema? ¿Por qué se lo digo? He mirado la memoria de la Fiscalía General del Estado de 2018. Criminalidad informática, son tres páginas, no se queja demasiado de este tema, pero en la parte de la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada, y la criminalidad organizada tiene mucho que ver con la cibercriminalidad, dice textualmente: Por otra parte, es una evidencia que existe un déficit de expertos informáticos en la fiscalía. En la actualidad solo uno, que debe atender a todas las incidencias que a diario se producen. Se trata de una cuestión que, sin duda, no solo afecta a la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada y que debe abordarse un nivel que permita redefinir las prioridades de una moderna oficina de la fiscalía. Está bien. En esta Comisión es común que las personas que comparecen digan que está bien pero que se necesitan más medios. Aquí la memoria de la fiscalía de 2018 lo dice paladinamente, pero en todo caso quería conocer su opinión como fiscal especializado.

Muchas gracias.

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

Señor Ramírez, para terminar este turno de portavoces.

El señor **RAMÍREZ RODRÍGUEZ:** Muchas gracias, señor presidente.

Señor Bermúdez, muchas gracias por su comparecencia, por los matices que ha traído a esta Comisión. Aunque no sé si debería darle las gracias o sentirme quejoso de todas las dudas que usted ha hecho planear sobre esta Comisión, incluso entra algo de pánico cuando uno ve la crítica tan grande que hace a cómo nos estamos defendiendo de esta gran amenaza de hoy, que no es la amenaza del futuro, como usted también muy bien decía. A lo largo de las comparecencias que se están produciendo en esta Comisión hemos sabido que normalmente hemos ido detrás de los ciberataques, es decir, que los instrumentos para defendernos van llegando después de que se vayan perfeccionando nuevos instrumentos de ataque, y uno tiene la sensación de que constantemente estamos perdiendo esa carrera. Más que matizar cada uno de los extremos y problemas que tiene todo lo relativo a la ciberseguridad, me referiría a ella de una manera global. Porque no arreglamos nada si, por ejemplo, conseguimos —como usted ha puesto de manifiesto— arreglar ese problema de que unas recomendaciones o sugerencias sustituyan la efectividad de un reglamento o la ausencia del Poder Judicial en lo que podría ser la instrucción de la comisión de delitos. Eso es muy importante, pero realmente no conseguiremos nada si atacamos cada uno de esos elementos por separado. Realmente, deberíamos abordar de una manera estratégica —incluso diría que con mucha más fuerza que hasta ahora— el problema de la ciberseguridad.

Se nos ha dicho también a lo largo de estas comparecencias que el Estado español se ha dotado de instrumentos muy útiles, de gran nivel y que en comparación con el resto de países de nuestro entorno, España es de los países más preparados para la ciberseguridad, y aún así, hemos visto con desazón cómo tenemos cinco autoridades para la notificación o cómo incluso hay alguna en forma de empresa, como usted ha criticado francamente muy bien. Creo que están a las puertas de Roma y que no tenemos soluciones definitivas. Da la impresión de que no nos pasan más cosas porque no se organizan suficientemente o porque los malos todavía no han querido que nos pasen más cosas.

cve: DSCG-12-CM-126

Le preguntaría: ¿Cómo resolvemos un instrumento legal, como tiene que ser el real decreto, cómo deberíamos resolver los reglamentos —que ahora mismo está siendo sustituido por sugerencias— y cómo deberíamos afrontar todo este problema de una forma global para ponernos la altura del ataque? Porque si no, estamos siempre por debajo de los atacantes, por muy bien que lo hagamos.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Tiene usted la palabra ahora.

El señor **BERMÚDEZ GONZÁLEZ** (fiscal delegado adscrito al Servicio de Criminalidad Informática de la Fiscalía General del Estado): Muchísimas gracias, señor presidente.

Voy a comenzar por el final, en orden inverso a la intervención de los distintos componentes de esta Comisión. Una cosa que quizás he dejado en el tintero es algo que está muy en boga ahora mismo en el mundo de la ciberseguridad, que es la seguridad ofensiva o seguridad activa. Se basa sobre todo en tres aes, tres iniciales que provienen del inglés: *annoyment, attribution* y *attack*. La primera de ellas es molestar, por utilizar el término de jerga en Internet, 'trolear' a los atacantes de tal manera que todo aquello que busquen no lo consigan. Si buscan un activo determinado de un sistema informático de una institución o de una empresa no lo consigan y estén dando vueltas sin obtenerlo. Esto, en principio, en completamente lícito —el despistar—; ahora bien, puede tener consecuencias realmente peligrosas. Por ejemplo, una empresa de gestión de tarjetas de crédito —esto es algo que me han contado directamente, se sabe que esto sucede— detecta determinadas microcompras —50 céntimos, 1 euro, puede ser una aplicación para teléfono móvil o una canción— de una serie de tarjetas de numeración correlativa. Dejan que esto se haga, no cancelan las tarjetas, no las anulan inmediatamente. ¿Por qué? Porque saben que en la *dark web*, en la parte oscura de Internet —que no es todo lo que nos han dicho, no es ese 90 % de Internet, sino un reducto bastante más restringido— alguien está vendiendo estas tarjetas que ha obtenido por exfiltración de datos de alguna fuente no autorizada. ¿Qué es lo que hacen? Esperan a que se hagan estas comprobaciones, porque lo que está haciendo el vendedor es comprobar que esas tarjetas siguen activas y, a continuación, las pone a la venta. Cuando las ha vendido, entonces las cancela. ¿Qué sucede? Que el que ha vendido estas tarjetas ha vendido un material defectuoso. Entonces, quizá haya algún vendedor de tarjetas falsas que esté con unos zapatos de cemento en el fondo del río Moskvá porque a la Bratvá, a la mafia rusa, no se le anda con tonterías y si le vendes tarjetas, tienen que funcionar. Estas represalias que adoptan determinados departamentos de ciberseguridad son llevadas a cabo por manos privadas. Pero el *annoyment* ya les he dicho que es en principio legítimo.

Attribution, obtener datos durante el ataque. Esto se lo planteé en una ocasión al magistrado excelentísimo señor Manuel Marchena, presidente de la Sala Segunda del Tribunal Supremo. Dije que el principio consolidado es que si alguien está hablando conmigo, puedo saber quién es mi interlocutor o puedo grabar la conversación. Si todo ataque se produce a través de una comunicación telemática y estamos hablando siempre de la protección del secreto de las telecomunicaciones, hay que aplicar el mismo principio. Si soy parte de la telecomunicación, tendré que poder utilizar mi posición no deseada de parte de esta telecomunicación para averiguar quién se está conectando a mis sistemas. Es decir, existen mecanismos jurídicos que nos permiten tomar un poco la delantera, ser preactivos, pero no se puede dejar que sean los particulares los que se tomen la justicia por su mano porque entonces estaríamos en el *Far West* y no en un Estado de derecho. Pero, como ve, herramientas tenemos y no cuestan dinero, es simplemente aplicar una visión transversal que integre tanto operadores jurídicos como operadores tecnológicos. Si nos ponemos de acuerdo, creo que podemos funcionar. Es un término que suena mucho en las charlas de los *coaches*, de los especialistas en motivación y la verdad es que a veces me produce cierta urticaria pero no deja de ser cierto, es una sinergia. Es decir, cuatro fuerzas actuando por separado no consiguen lo mismo que si esas cuatro fuerzas se convierten en un ciclo que, al final, hace una rueda y es capaz de transmitir muchísima más fuerza.

Daniel de Ugarte, que era el autoproclamado ideólogo del movimiento ciberpunk español, allá por principios de este siglo, escribió un libro titulado *11M. Redes para ganar una guerra*, que tiene un corolario que me encanta, y es que las redes se combaten con redes. Si precisamente hemos tenido un problema en la implementación de este real decreto-ley ha sido la dispersión de autoridades, porque ya son autoridades preexistentes. El CNPIC ya existía antes, el CCN-CERT ya existía antes y el Incibe ya existía antes. De hecho, recordarán que Incibe nace como Instituto Nacional de Tecnologías de la Comunicación, cuando era conocido como Inteco. Y es posteriormente, cuando pasa a asumir esta nueva identidad.

cve: DSCG-12-CM-126

Míster Proper ahora se llama Don Limpio e Inteco ahora se llama Incibe y es el Instituto Nacional de Ciberseguridad. Yo he tenido el inmenso placer de ser profesor en las jornadas de la escuela de verano, el Cibersecurity Summer BootCamp, que organizan en los meses de julio, y les puedo decir que son jornadas apasionantes en las que se comparte conocimiento por parte de operadores jurídicos, tecnológicos, policiales y abogados. Hay cuatrocientas personas trabajando en común para conseguir soluciones en este sentido. Incibe no es una institución con la que yo sea crítico, todo lo contrario, lo que digo es que quizá la están obligando a ser algo que no es.

¿Medidas concretas? Coordinación. Llámelo una secretaría de Estado de ciberseguridad, no tanto un ministerio. En Japón hay un ministerio de ciberseguridad que, por cierto, el titular de la cartera en su presentación dijo que no sabía ni encender un ordenador. Bueno, espero que sea muy bueno como ministro porque, desde luego, como tecnólogo él mismo reconoce que no vale para nada. Quizá una secretaría de Estado o una subsecretaría de Estado, dependiente de alguno de los ministerios que ya están llevando competencias en la materia. Se me ocurre, sin ir más lejos, hablando de Incibe, la Secretaría de Estado de Avance Digital. Entre el director general de Incibe y la Secretaría de Estado de Avance Digital hay un vacío administrativo en el que podría caber una subsecrertaría de Estado de ciberseguridad, con competencias transversales que aglutinaran. También es cierto que el CNPIC depende de la Secretaría de Estado de Seguridad. Siempre estamos con lo de defender las competencias propias, este prurito de 'es mi agencia', pero yo entiendo que más de apropiarnos de recursos de otros, lo que tenemos que hacer es coordinarlos y tiene que haber alguien que haga la coordinación. Porque una red tiene que tener nodos; sin nodos una red no es más que un grupo de actores dispersos. Así que yo creo que más que una inversión multimillonaria en comprar los últimos ordenadores, necesitamos actuar con cabeza y tomar medidas concretas en relación con esta cuestión, que no cuestan dinero, cuestan únicamente un esfuerzo por colaborar, por generar una sinergia, por establecer unas redes de cooperación para dar una respuesta unitaria; que cualquier persona que quiera denunciar algo relacionado con un incidente de ciberseguridad se encuentre con un único interlocutor, no con cinco ni con una ruta de denuncia que pueda ser como completar una *gymkana*.

En cuanto a las preguntas que me plantea el señor Hernando, en primer lugar, le tengo que dar las gracias por comprar mi libro. Quizá así algún día vea algo de lo que me corresponde como coautor del mismo. Lo cierto es que ya saben cómo son estas cosas, uno escribe por amor al arte; realmente, ustedes lo saben mejor que nadie, lo mismo que yo como jurista, la ley no tiene derechos de autor, los escritos presentados ante los tribunales no tienen derechos de autor. Internet, como me imagino que les habrá dicho el doctor De la Cueva, está basado en una estructura libre de propiedad intelectual, fue una donación a la humanidad, se basa en *software* libre; así que los juristas tenemos que estar muy acostumbrados a convivir con el *software* libre, porque básicamente se basa en altruismo, en querer colaborar con la comunidad a cambio de nada. Yo no cobro absolutamente ningún *royalty* por los escritos de acusación que presento ante los tribunales; lo mismo que ustedes no cobran ningún *royalty* por el hecho de que una ley sea citada una y otra vez. Pues bien, el *software* libre, la comunidad de *software* libre que está interesada en contribuir, existe; la cuestión es que las empresas informáticas no se llevan la parte del león de las inversiones, sino que se la llevarían informáticos que son los que operarían sobre el terreno y nos permitirían tener una asistencia técnica más cualificada. Pagamos un pecado original y es el de las dependencias. Yo creo que en el futuro una profesión con salida será la paleoinformática. Habrá que encontrar un dispositivo que sea capaz de leer un disco flexible, un disquete de cinco pulgadas y cuarto o un disquete semirrígido de tres pulgadas y media. Dentro de veinte años, un disco duro de los que conocemos hoy en día será algo raro de ver. De hecho yo he tenido problemas con discos duros antiguos que utilizaba y que usaban un puerto de comunicaciones distinto que ya no se utiliza.

Digamos que tenemos herramientas, atendiendo a su pregunta sobre la Administración de Justicia, como Lexnet, que provienen de un desarrollo muy anterior en el tiempo, y como son operadores, quiero pensar que críticos —la justicia—, no hemos podido aparcarlos para construir uno nuevo, le hemos ido añadiendo parches. El hipervisor Horus, el Portafirmas, la conexión con el sistema judicial Minerva, son cosas que, francamente, no he tenido la oportunidad de tocar porque vivo en el País Vasco y el hecho diferencial vasco, entre otras cosas, supone que tenemos un sistema de gestión procesal informático propio llamado JustiziaBat. Está bastante más retrasado en cuanto a su implementación en fiscalía y, por ello, doy gracias todos los días al levantarme, porque lo que me transmiten mis compañeros es que trabajar con la fiscalía digital es un dolor. Y una parte importante de las reivindicaciones que se han hecho por parte del colectivo judicial y fiscal es eliminar esta fiscalía digital y partir de cero. Entiendo que quizá

cve: DSCG-12-CM-126

no sea posible, porque hay una inversión previa, hay unos sistemas desarrollados, pero sin duda hay que hacerlos muchísimo más ágiles para que sirvan a su función. Quizá hay que concienciar a los informáticos que los diseñan o que trabajan con ellos de que no somos una empresa de informática, cuyo usuario final es un señor que lleva una toga negra muy rara con una especie de trozo de cortina en la bocamanga. No, somos la Administración de Justicia, es la informática la que está a nuestro servicio, no nosotros al servicio de la informática. Quizá es ese cambio de mentalidad y de paradigma el que hay que hacer.

En cuanto a doña Elvira Tejada, qué voy a decir si desoyeron sus recomendaciones. Muy mal, señorías. Líbreme el Altísimo de desoír a la que no es mi superior jerárquica, porque mi superior jerárquica es la fiscal provincial de Guipúzcoa, pero funcionalmente, como miembro de la red de criminalidad informática, sí que es mi superiora absoluta. Y, por supuesto, en absoluto, jamás, dejaría caer en saco roto ninguna de sus recomendaciones. Así que si no la hicieron caso, pónganse las pilas, porque les aseguro que doña Elvira sabe muy bien de lo que habla, porque no en vano lleva desde 2011 allí e incluso desde antes ha tenido contacto con estas responsabilidades. Así que, siquiera sin necesidad de volver a ver su ponencia, que por supuesto vi en su día, no puedo decirles más que hago suyas sus recomendaciones plenamente.

Medidas concretas, ¿qué hacer? Bueno, ya les he dado algunas ideas que son más una ocurrencia propia, una mente que intenta pensar de forma lateral; lo que les he dicho antes, pensar fuera de la caja. Me gusta mucho un concepto que aparece en una novela de Max Brooks, *Guerra Mundial Z*, que es la del décimo hombre, y es la de que cuando nueve personas piensan igual, tiene que haber un décimo que piense en contra de todos los demás, para asegurarse de que no se produzca ese tradicional resultado de que cuando todos piensan lo mismo es señal de que alguien no está pensando. Bueno, pues alguien que lleve la contraria por sistema. Muchas veces estará equivocado y nos felicitaremos por ello, y le diremos: ¿Ves cómo esta vez te habías equivocado? Pero cuando realmente acierte, que estemos prevenidos. Por eso he hecho estas sugerencias que, dentro de lo que cabe, no caen dentro de mis competencias, porque —como les he dicho— soy un fiscal de una fiscalía provincial y líbrenme de todos los males de hacer ningún tipo de sugerencia al legislador de por dónde tienen que ir sus trabajos. No me considero con autoridad moral ni conocimiento suficiente para ello orgánicamente, como fiscal; ahora bien, como estudioso de la materia, ya he lanzado algunas ideas concretas de lo que se podría hacer.

Mencionaba precisamente el capítulo de este libro en el que tuve el orgullo de participar, que entiendo que es un manual de cabecera sobre el desarrollo jurídico de la investigación tecnológica, y decía que, efectivamente, las calles de Internet no se parecen a las calles de Madrid; se parecen más bien a las escaleras de Hogwarts, la escuela de magia y hechicería, en el sentido de que están cambiando constantemente y, hoy, la escalera que te lleva aquí dentro de tres segundos te lleva allí.

Nuestra experiencia con los Gafam, particularmente con Google y Microsoft, si se les piden cosas poco invasivas, una dirección IP desde la que se creó un correo electrónico, responden con bastante rapidez; colaboran, digamos que porque no les molestamos mucho. Ahora bien, como les pidamos el contenido de un buzón de correo electrónico o de ciertas fotos almacenadas pero no visibles para la mayoría de los ciudadanos, entonces ya utilizan el viejo dicho de español antiguo de 'llamarse andana'. Se acogen a sagrado y dicen: soy una empresa estadounidense —aunque cuando me interesa no tengo sede social en Estados Unidos, sino en Luxemburgo, pero como ahora me interesa tengo mi sede en Estados Unidos—, así que me acojo a la legislación norteamericana. Así que si ustedes quieren eso, pídanme una comisión rogatoria. La comisión rogatoria para cuando se traduce, se envía y sigue todos los trámites ya no sirve absolutamente para nada porque ha tardado dos años en cumplimentarse. Es así de triste. Twitter es particularmente bastante reticente a dar datos. Se han dado muchísimos casos de suplantación de identidad utilizados para difundir bulos y falsos rumores o, simplemente, para ridiculizar a personajes públicos y Twitter se niega a darnos información. Ahora parece que empieza a colaborar algo más, empieza a dar alguna dirección IP. También se han dado cuenta de que utilizando herramientas de inteligencia de fuentes abiertas la policía puede conseguir resultados que no dependen únicamente de una dirección IP. Simplemente cruzando datos pueden obtener un resultado que va mucho más allá de lo que nos podría decir la dirección IP desde la que se produjo la conexión. Es un problema territorial, de nacionalidad, de soberanía, de, en definitiva, estar anclados en viejos arquetipos, cuando hemos evolucionado hacia otro estado. Insisto, estas empresas siguen agarrándose a ellos cuando les conviene.

En cuanto a la reforma de la Ley Orgánica 1/2015, tendría que ser otra ley orgánica la que procediera a reformar el Código Penal. Creo que tenemos suficientes ejemplos en el código de delitos en los que existe una exención de punibilidad, en la que no se castiga al responsable. Sin ir más lejos, por ejemplo, el cohecho, cuando se procede a denunciar este intento de soborno a un funcionario público; el delito de

cve: DSCG-12-CM-126

fraude tributario, cuando la persona que ha sido objeto de una inspección regulariza su situación tributaria antes de que el procedimiento se dirija contra él queda exento de responsabilidad criminal; e incluso en las lesiones, las lesiones mutuamente consentidas en principio tienen una rebaja de la pena, pero cuando se trata de cirugía de esterilización de personas discapacitadas no hay responsabilidad penal para el médico que la práctica. Asimismo, la famosa Ley de Interrupción Voluntaria del Embarazo o Ley del aborto no es más que la despenalización de una conducta que estaba castigada. Por lo tanto, habría que arbitrar alguna medida de exención de punibilidad para aquella persona que, habiendo obtenido acceso a un sistema de la información, proceda inmediatamente a advertir a las autoridades o a los titulares legítimos del sistema de esta vulnerabilidad para que sea corregida, sin intentar obtener ningún aprovechamiento personal directo o indirecto. Entiendo que esto les daría un cierto nivel de seguridad jurídica que, por otro lado, tienen en Estados Unidos, donde está institucionalizada la figura de las *bug bounty*, el botín por encontrar una vulnerabilidad, o en la misma Unión Europea. La Unión Europea acaba de sacar un programa de recompensas para catorce o quince herramientas de *software* libre que permiten que los ciudadanos libremente las auditen para buscar vulnerabilidades y reportarlas. Por supuesto, no va a haber ninguna consecuencia perjudicial, sino todo lo contrario, esto va a ser recompensado, aunque no sé exactamente de qué manera, si moralmente con una mención o si va a haber algún tipo de estipendio. En Estados Unidos y en otros países como Japón es habitual el premio económico. Yo no estoy diciendo tanto, no te pido que me regales, pero por lo menos no me persigas. No me pagues o págame, si al final mis servicios son bastante avanzados, pero, por lo menos, no me hagas objeto de una persecución penal. Eso sería bastante interesante y creo que la comunidad de ciberseguridad lo agradecería. No ir tanto con el palo o el martillo, sino que, de vez en cuando, usar la zanahoria, es mucho más agradable y provoca muchos menos enfrentamientos.

Respecto a lo dicho por la representante del Grupo Parlamentario Confederal de Unidos Podemos, esta paranoia a la que ha hecho referencia me recuerda a un dicho que utilizo muchas veces con mis estudiantes, con mis alumnos de algún curso o con los asistentes a alguna ponencia. Para mí el paraíso es donde viven los abogados de la defensa: ese muerto ya estaba ahí, señoría; esas drogas no son de mi cliente; las lesiones nunca fueron tan graves; los daños, en realidad, son mera responsabilidad civil y todo esto no es tan grave. Ese es el paraíso. ¿Cuál es el infierno? El infierno es donde viven los especialistas en seguridad informática: todo es vulnerable, todo es atacable; si mi ordenador arranca una décima de segundo más tarde es que algo le pasa. Conozco a informáticos que son capaces de destripar su equipo solo porque de repente funciona un poco más lento. Esto me recuerda a una película protagonizada por Gene Hackman y dirigida por Francis Ford Coppola hace ya décadas, *La conversación*, en la que un experto en escuchas de la CIA acaba destripando su propio apartamento porque sospecha que hay un micro. Entre Pinto y Valdemoro, ni tanto ni tan calvo. Vamos a encontrar un sano equilibrio y un sano sentido común de ni todo es tan grave ni hay que vivir en un estado de todo es perfecto y bonito y nunca pasa nada; que tampoco es así.

La falta de presencia de los operadores jurídicos en el mundo de la ciberseguridad es, efectivamente, muy preocupante porque el Estado de derecho se basa en un Poder Ejecutivo, un Legislativo y un Judicial. Ya dijo el barón de Montesquieu —en gloria esté— que no hay peor dictadura que la del que hace las leyes y, además, se encarga de imponerlas o la del que hace las leyes y, además, se encarga de juzgarlas, y si juntamos estos tres poderes en uno solo, tenemos la dictadura más absoluta. Por tanto, sigo creyendo en la separación de poderes y, por supuesto, sigo creyendo en el Poder Judicial como una de las columnas fundamentales de todo Estado de derecho. Por tanto, ¿qué podemos hacer con la presencia de operadores jurídicos? Pues aprovechar este trámite parlamentario de trasposición del real decreto-ley para darle mayor participación a la fiscalía. Hay un órgano que me interesa muchísimo y es la Dirección de Seguridad Nacional porque tiene varios comités bajo su dependencia que forman órganos de trabajo permanentes y uno de ellos es la Comisión Nacional de Ciberseguridad. Entiendo que Justicia debe tener presencia en ese Consejo Nacional de Ciberseguridad para, precisamente, poder dar criterios jurídicos. En Estados Unidos el *attorney general*, el fiscal general del Estado, no es solo el jefe de todos los fiscales federales, sino que, además, es el asesor jurídico del Gobierno. Sería impensable tomar una decisión en materia de seguridad nacional sin contar con el *attorney general*. Por tanto, desde el punto de vista del conocimiento que pueda tener la fiscalía en materia de persecución del cibercrimen y de lucha por la ciberseguridad, contar con la fiscalía y con sus especialistas sería interesante en este Consejo Nacional de Ciberseguridad.

En cuanto a la formación, requiere presupuesto. En ese sentido, sé que puede sonar a queja repetitiva, pero es cierto que la justicia es siempre el pariente pobre en los Presupuestos Generales del Estado. Por

cve: DSCG-12-CM-126

tanto, quizás un pellizquito en materia de formación nos ayudaría a que los cursos se pudieran pedir, porque existen. También deberíamos tener en cuenta que los cursos, cuando se piden, hay que poder acudir a los mismos. Muchas veces hay jueces y fiscales que piden cursos pero tienen que renunciar a ellos porque, de repente, tienen señalamientos que no pueden suspender porque si el juicio no se celebra hoy, 23 de enero de 2019, quizás el único hueco libre que haya en la agenda sea en febrero de 2021 y una justicia tardía no es justicia. Estos profesionales, por un prurito de profesionalidad, precisamente, renuncian a su formación para poder cumplir con su función. El problema es que esto es como el miembro que se gangrena, al final tenemos que permitirles que se liberen en cierta medida de esta carga de trabajo para poder acudir a esos cursos de formación porque si no, al final, sabrán lo que sabían hace veinte años y eso no servirá. Hace falta tener conocimientos mínimos en materias relacionadas con ciberseguridad, aunque solo sea para autoprotección de los jueces y fiscales. Una de mis primeras intervenciones en la recién constituida Red de fiscales de criminalidad informática, allá por 2012, a petición de doña Elvira Tejada, fue sobre unas breves nociones de qué necesitaríamos para protegernos de intrusiones informáticas. Enumeré una serie de cosas que, por aquel entonces, podemos decir que eran el *state of the art*, el estado de la ciencia en aquel momento, en materia de seguridad para fiscales y jueces. El presupuesto, a mi modo de ver, era risible, era el chocolate del loro. Sin embargo, el Ministerio de Justicia no tuvo a bien en aquel entonces destinar una partida presupuestaria para estas necesidades. Exactamente dos años después se hicieron públicos varios agujeros de seguridad informática que afectaban a la Fiscalía de lucha contra la corrupción y el crimen organizado en varias causas relacionadas con criminalidad organizada de muy alto nivel, mafias rusas y otros casos de mucha más proyección mediática que quizás no sea el momento de hablar de ellos. Sí, había serios problemas con la ciberseguridad en las fiscalías. Que digan que solo tienen un informático en anticorrupción, que es el ojito derecho de la fiscalía… Imagínese cómo estamos en las fiscalías provinciales. La pregunta más habitual que tengo que escuchar es: ¿Eres el fiscal de Criminalidad Informática? Sí. La impresora no funciona. **(Rumores).** Somos el chispas; tenemos ciertos conocimientos informáticos, así que tenemos que suplir muchas veces al centro de atención al usuario, que a veces está sobrecargado y es más fácil decir: compañero, el teclado no funciona. ¿Has probado a comprobar si está bien enchufado? Frecuentemente funciona esta recomendación.

En cuanto a cómo podemos adaptar las tecnologías de la información a la Administración de Justicia, creo que ya he dado por contestada esa pregunta: mediante una inversión que, sobre todo, adapte lo que ya tenemos porque empezar desde cero probablemente sea inasequible.

En cuanto a los delitos contra la intimidad, están muy bien regulados en el Código Penal; de hecho, suelen ser de los que más desarrollo de investigación tienen porque, al final, una persona que distribuye pornografía infantil a través de una red de intercambio de archivos es relativamente fácil de identificar, el problema es cuando estamos persiguiendo a alguien que ha compartido un vídeo de una persona manteniendo relaciones sexuales sin su consentimiento, que ha sido grabada sin su consentimiento, localizar el origen de esa grabación, aunque se consiguen muy buenos resultados. La verdad es que yo he llevado algunos casos en la Fiscalía Provincial de Guipúzcoa con buen resultado, con un trabajo policial extraordinario, bien de la Ertzaintza, bien de la Policía Nacional o de la Guardia Civil, y hemos conseguido buenos resultados. Esos delitos contra la intimidad realmente son, no diré de los que menos me preocupan porque me preocupa todo, pero de los que menos me quitan el sueño.

En cuanto al Internet de las cosas, evidentemente ha venido para quedarse y no se va a ir. Quizá sería más bien competencia del Ministerio de Industria: exigir a los fabricantes que tengan la privacidad y la seguridad por defecto en su diseño. De hecho, es uno de los mantras de los expertos en ciberseguridad. En informática al final hay dos tipos de mentalidades: la mentalidad de ingeniero, que es el 90% de los que se dedican a esto, que es hacer algo y que funcione, y la del experto en ciberseguridad, que es, si funciona, a ver por dónde se rompe y si al romperse me permite hacerme con los mandos del invento. Entonces, quizá hay que tener en cuenta a estas personas, no relegarlas al último escalón jerárquico, y exigir a las empresas un nivel de seguridad por defecto que precisamente es de lo que habla el Reglamento Europeo de Protección de Datos, privacidad y seguridad por defecto. Es el punto de vista desde el que tenemos que partir y, de hecho, contempla sanciones estratosféricas en términos económicos, de hasta el 2% o el 4% de la facturación de una empresa. Quizá el sonido del efectivo escapándose de sus bolsillos sea una señal de atención para estas empresas. Así que en ese sentido habría que dar un serio toque de atención porque lo que no es de recibo es que se pueda acceder a través de un *malware* a múltiples cámaras de seguridad simplemente porque no tienen usuario y contraseña. Al final lo que no podemos

cve: DSCG-12-CM-126

hacer es el *user shaming*, avergonzar al usuario. El usuario no es el culpable de que le vendan un producto inseguro. Es como, *mutatis mutandis* —permítanme la licencia literaria—, culpar a una víctima de un delito sexual de haber ido con la falda muy corta. Esto es algo que a nadie se le ocurre hoy en día. **(La señora Angustia Gómez: ¡Bueno!).** Sí, bueno, puede que haya algún carpetovetónico que todavía lo piense, pero en el imaginario colectivo ya está suficientemente establecido que lo que los yanquis llaman ese *look shaming* es intolerable. Por la misma razón, yo creo que en materia de bienes de consumo electrónico no podemos caer en el *user shaming*, es decir avergonzar, victimizar o culpabilizar al usuario al que le han dado un producto inseguro por defecto.

En cuanto a las criptodivisas, uno de los comparecientes en esta Comisión, don David Maeztu Lacalle, letrado en ejercicio, es uno de los mayores expertos nacionales en materia de régimen jurídico de criptodivisas, de criptoactivos porque, en realidad, ni son monedas ni son divisas. Sí me preocupa mucho su utilización para el *money laundering*, el blanqueo de capitales o el lavado de activos, como dicen en los países hispanoamericanos —recientemente estuve en Ecuador en una actividad de cooperación internacional y ellos lo llaman el lavado de activos—, pero no porque sean diseñados para el mal. De hecho, el *blockchain*, la cadena de bloques, que es la tecnología que subyace a estos criptoactivos, es una herramienta que se está pensando en utilizar para otros muchos fines; de hecho, quizás estamos empezando a vender humo en cuanto a lo que puede conseguir el *blockchain*, dicen que si van a sustituir a los notarios y a los registradores porque dan una mayor garantía de determinados hechos. Sí, y también pueden decir que va a curar el sida, el cáncer y va a solucionar el hambre en el tercer mundo. Seamos realistas. Sirve para garantizar que una determinada cosa ha sucedido porque permite que múltiples operadores de confianza garanticen que sí, que ha sucedido. Así es como se producen los asientos contables en las transferencias de criptoactivos. Es una tecnología que se puede ampliar a otros usos, que es muy útil, pero hay que tener en cuenta no solo los bitcoins, que es, digamos, la madre del cordero en esto de los criptoactivos, sino todas las monedas o activos que están derivando y que tienen una finalidad esencial de ser irrastreables. En ese sentido, la cooperación internacional es muy importante. Allá donde haya un puerto seguro para poder conseguir criptoactivos sin necesidad de dar datos personales va a haber una fuente de fraude y no lo podemos evitar, pero la utilización de fuentes abiertas de información, la inteligencia policial, consigue resultados muy positivos en esta materia y tenemos casos policiales en el último año muy sonados en materia de detención de responsables de delitos de este tipo.

Termino con las preguntas que me ha dirigido el responsable de Ciudadanos. En cuanto al *total free*, ya lo he dicho antes, al comienzo de Internet la gente era más altruista, luego entraron los comerciantes y buscaron una monetización de todo, pero al final se puede conseguir monetizar sin recurrir a esquemas antiguos. El *software* libre puede producir beneficios económicos. Lo que sí es obsoleto es, por ejemplo, pretender obtener un beneficio de la venta de trozos de plástico como los CD. Mi hijo ya no sabe lo que es un CD y menos aún un CD-ROM. Nunca ha visto que un ordenador de su padre tenga lector de CD-ROM ni lector de DVD. Así que los esquemas clásicos de propiedad intelectual de *software* basados en la venta de piezas de plástico quizá estén realmente obsoletos y tendríamos que fijarnos en las compañías que han conseguido monetizar el *software* libre como, por ejemplo, Red Hat, la compañía que ha creado Ubuntu, un sistema operativo completamente libre, y que yo creo que es una compañía bastante saneada que no tiene ningún problema. De otro lado sacará sus ingresos, probablemente sea de la asistencia técnica porque si es un sistema operativo que no está tan difundido, no lo sabe manejar todo el mundo. Aunque realmente, viendo Windows, no todo el mundo sabe manejarlo. Hará falta, si no es una inversión en licencias de sistemas operativos, una asistencia técnica que nos ayude con estos problemas y yo creo que será incluso más productivo porque liberará activos presupuestarios de malgastarlos en sistemas cerrados de los que no tenemos conocimiento y nos permitiría tener un *software* que pudiéramos auditar y controlar.

En cuanto a la gobernanza de Internet y el papel de la justicia, como ya les he dicho antes, entiendo que la creación de algún tipo de organismo de coordinación en materia de ciberseguridad, llámese secretaría de Estado o subsecretaría de Estado, el nombre que quiera dársele, que aglutine o, sobre todo, que coordine, no que pretenda atraerlos a todos para gobernarlos en las tinieblas como el Anillo Único, sino que lo que busque sea una coordinación proactiva de todos los grandes activos que tenemos y que en lugar de ser cuatro fuerzas centrífugas, sean una sinergia que nos permita que la rueda se mueva.

En cuanto a las *fake news*, los bulos, el *fact checking* es una de las técnicas más en boga hoy en día. Da mucha fuerza contraponer a los bulos la información contrastada y permite combatir esto. De hecho, ahora mismo una de las principales preocupaciones del Consejo Nacional de Ciberseguridad es combatir

cve: DSCG-12-CM-126

estas *fake news*. ¿Qué pasa cuando se trata de bulos que afectan a una única persona, a un particular? Evidentemente, una denuncia ante un órgano judicial es una lotería y quizá por eso lleva siendo el mantra que escucho desde que empecé la oposición, y hace más años de los que quiero acordarme y ya mis preparadores lo habían oído en aquel entonces, era el cambio del modelo de instrucción penal con una fiscalía como director de la investigación que permitiera que fiscales especializados en una materia pudieran hacerse cargo de ella allá donde estén destinados, sin necesidad de que el juez sea una especie de maestro de todo, que es imposible, no pueden saberlo absolutamente todo. Así que la facultad de especialización que ofrece el ministerio fiscal, siempre con el debido control de la autoridad judicial, del juez de garantías, sería quizá el paso que habría que adoptar, pero habría que adoptarlo bien, con medios suficientes para que la fiscalía pudiera hacerse cargo de la instrucción, no simplemente con un traspaso de competencias en bloque que dejaría a los juzgados sin trabajo y con un exceso de funcionarios, y a las fiscalías completamente desbordadas y enterradas en papel, que es lo que desgraciadamente seguimos manejando a día de hoy.

Lo siento si les he planteado más dudas que certezas. Al final, como decía Heidegger, aquel que no se cuestiona a sí mismo según se levanta, sin duda no merece la pena y yo tengo por costumbre cuestionarme todo lo que sé y todo lo que expongo. Espero, por lo menos, haber solucionado algún problema más de los que he planteado.

Nada más. Muchas gracias.

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

Son las tres y diez de la tarde y hay un segundo turno. Apelo al buen sentido de sus señorías y no ya al reglamento, que son tres minutos.

Señor Salvador.

El señor **SALVADOR GARCÍA:** En primer lugar —y brevemente, como ha dicho el presidente, dada la hora—, le vuelvo a felicitar. Creo que nadie ha tenido la sensación de que nos haya trasladado problemas. Estamos aquí unos y otros para decir qué es lo que no está funcionando, qué se puede corregir y qué se puede optimizar y, por lo tanto, todo lo que ha dicho me parece absolutamente coherente. Lo que sí digo es que se ha evidenciado algo que lleva pasando desde el origen de la sociedad de la información y que hoy ha pasado con varios comparecientes, y es que todavía no hay plena integración del mundo digital con el mundo analógico en las cabezas de quienes tienen que identificarlo, algo que yo decía siempre: hay gafas del siglo XX y gafas del siglo XXI. Quien tiene puestas las gafas del siglo XX y analiza un problema del siglo XXI seguramente no sabrá solucionarlo o producirá un efecto adverso. Por tanto, tenemos que armonizar y que haya unas gafas únicas, porque si no esto pasará en la justicia, pasará en la política o en cualquier ámbito donde haya que tomar una decisión.

Cuando he hablado de la gobernanza no me refería tanto a Internet sino a lo que usted ha dicho respecto al tema de ciberseguridad. Y en cuanto a lo del *total free* tampoco me refería al altruismo sino a que como no ocuparon ese espacio quienes trabajaban desde el negocio, se fomentó el compartir conocimiento y después, cuando entraron, dijeron: oye, hay que poner un nuevo modelo de negocio. Y en esto igual, como había que tomar medidas urgentes en cuanto al concepto de ciberseguridad, se han creado organismos y ha habido una organización de defensa, pero ahora que estamos en un momento ya maduro, hay que tomar decisiones y saber qué papel tiene que ocupar cada cual y, a partir de ahí, ver cómo se tienen que coordinar, y estoy de acuerdo en lo que usted ha sugerido sobre la creación de un organismo desde el ministerio que sea el que lo coordine todo.

Muchas gracias.

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

Señora Angustia.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente. Intervendré de la forma más breve que sea capaz.

Ha mencionado a Ecuador de pasada durante su intervención y fue precisamente el ejercicio profesional como fiscal el que lo llevó allí a trabajar en el Programa de Asistencia contra el Crimen Transnacional Organizado. Nosotros tenemos una relación natural con América Latina, pero muy pocas veces hablamos desde el marco del ciberespacio de esta relación. Hay otro espacio, al que también le ha llevado el trabajo en la fiscalía y con el que ya no tenemos una relación tan natural —como no es objeto

cve: DSCG-12-CM-126

de esta Comisión no voy a pasar a analizarlo—, que son algunos países de Oriente Medio; también ha trabajado allí en su ejercicio profesional, en la fiscalía. Me interesa, en ambos sentidos y de forma muy breve, todo lo que pueda ser materia —por lo menos me gustaría que la esbozara— de ciberseguridad, que es la única actividad que nos trae aquí, y que pueda ser susceptible de generar espacios de trabajo o interés en torno al tema en la ponencia que nos queda por delante.

Muchas gracias por todas las aportaciones, que yo también creo que han sido positivas. No solo nos ha resuelto dudas sino que además nos ha hecho propuestas. Muchas gracias por su disponibilidad para estar aquí y por todas esas aportaciones.

El señor **PRESIDENTE:** Gracias, señora Angustia.
Señor Hernando.

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

Señor Bermúdez, en esta entrevista que les hacen a ustedes, al fiscal Zaragoza y a usted, con motivo de un caso que llevaron para evitar la incitación al suicidio de menores, en concreto de una menor residente en Guipúzcoa, a la pregunta de si consideraba que deberían crearse juzgados y órganos especializados en criminalidad informática la respuesta fue: Desde luego. La pregunta en mi caso es: ¿se ratifica y eleva a definitiva esa conclusión?

El señor **PRESIDENTE:** Gracias, señor Hernando.
Señor Rodríguez.

El señor **RODRÍGUEZ-COMENDADOR PÉREZ:** Gracias, señor presidente.

Señor Bermúdez, muchísimas gracias por su comparecencia de hoy, por habernos abierto mucho más los ojos, y yo desde luego coincido con usted en que en este quinto escenario sin duda estamos en los albores de los tiempos. Nos queda muchísimo por ver y todo por aprender.

Gracias.

El señor **PRESIDENTE:** Señor Bermúdez, tiene la palabra para cerrar.

El señor **BERMÚDEZ GONZÁLEZ** (fiscal delegado adscrito al Servicio de Criminalidad Informática de la Fiscalía General del Estado): Señor presidente, cuando un operador jurídico dice que será breve normalmente suele ser mentira. Como estoy en las Cortes, procuraré hacer honor a la verdad. Y las gracias las debo dar yo por haber tenido esta increíble oportunidad.

Respecto de la intervención del representante de Ciudadanos, tengo que entonar el *mea culpa*. Ahora que he unido esas tres cuestiones que ha planteado he visto el encaje que tenían y coincido completamente con su visión.

En cuanto a la intervención de la representante de Unidos Podemos, diré que Ecuador tiene una característica de la que yo he hablado aquí: la instrucción se lleva por la fiscalía. Sin embargo, lo cierto es que tienen bastantes problemas de implantación porque su modelo está a caballo entre el modelo estadounidense y el modelo continental, es decir, siguen teniendo una judicatura muy fuerte que plantea muchos problemas a los fiscales investigadores y luego los investigadores civiles de la fiscalía no tienen la consideración de agentes de la autoridad. Es un sistema interesante de investigar. Su legislación está muy preparada en materia de ciberdelincuencia en el plano sustantivo y quizás les falte alguna pequeña actualización en materia procesal. Espero que pasen a formar parte del Convenio de Budapest de Ciberseguridad.

Con relación a los Emiratos Árabes, hubo una conferencia de ciberseguridad y ciberdelincuencia en la que tuve que sustituir a doña Elvira Tejada porque le resultaba imposible acudir, y mi sorpresa fue que cuando yo hablaba de garantías constitucionales, derechos fundamentales y problemas procesales, aquellas buenas personas me miraban como quien ve a extraterrestres. Digamos que sus sistemas jurídicos son notablemente menos garantistas. Lo que importa es que esté previsto en la ley y cómo cogemos al delincuente, lo demás les trae bastante sin cuidado, con lo cual fue un choque cultural bastante intenso. Eso sí, lo que tienen es capital, dinero y fondos para invertir hasta aburrir. Si hace falta tener lo último, lo van a tener a la voz de ya.

En cuanto a la intervención del señor Hernando, me causa dolor que me recuerde ese caso porque finalmente esa persona se suicidó un año y pico después. Además, me causó desagrado que mi compañero Zaragoza, que fue quien llevó el caso, tuviera que enfrentarse y dar explicaciones por haber

cve: DSCG-12-CM-126

intentado acelerar todos los trámites lo máximo posible, con lo cual se saltó ciertos requisitos jerárquicos, pero en su momento, cuando lo hizo, lo que consiguió fue salvar una vida.

Respecto a si hay que crear órganos especializados, sí, sin duda. ¿Sean juzgados o sean fiscalías? Mientras no sea la fiscalía la directora de la instrucción, yo creo que el modelo en el que debemos fijarnos es el de los juzgados de Violencia sobre la Mujer, porque desde el momento en que entra una persona con una denuncia en veinticuatro horas se va con una resolución que puede incluir una orden de protección, una prohibición de acercamiento, una prohibición de comunicaciones y una batería de medidas civiles y administrativas; o sea, reacción inmediata. Si hay órganos judiciales que tengan que llevar estas materias de forma especializada tienen que actuar como los CERT, como los centros de respuesta temprana; no se puede dejar para dentro de seis meses porque dentro de seis meses la información no va a estar disponible. Evidentemente, si es la fiscalía la que dirige la investigación, como fiscal especializado me sentiré muchísimo más realizado.

Nada más.

El señor **PRESIDENTE:** Muchísimas gracias.

Se levanta la sesión.

Eran las tres y veinte minutos de la tarde.

cve: DSCG-12-CM-126