DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2017 | XII LEGISLATURA | Núm. 73 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 12

celebrada el jueves 14 de diciembre de 2017 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

---

cve: DSCG-12-CM-73

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

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

— DEL SEÑOR SARTS, DIRECTOR OF THE NATO STRATCOM CENTER OF EXCELLENCE, PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/000926 y número de expediente del Senado 715/000308).

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

Vamos a dar comienzo a la sesión de la Comisión Mixta de Seguridad Nacional, que tiene dos comparecencias. La primera la de don Janis Sarts, director de NATO STRATCOM, y la segunda la de doña Elvira Tejada de la Fuente, fiscal de la Sala Coordinadora en materia de criminalidad informática. Esta no es la primera de las sesiones que dedicamos a un tema en el que están interviniendo y tomando parte todos los Parlamentos del mundo y les pareció interesante a la Mesa y a los portavoces que esta Comisión se interesase también por lo que está ocurriendo. En primer lugar, doy la bienvenida al señor Sarts, *very welcome to Spain*. Tendrá una comparecencia por el tiempo que considere oportuno. A partir de ahí, abriremos una primera ronda de intervenciones por parte de los portavoces de los distintos grupos parlamentarios. Habrá una segunda intervención, que se cerrará con una intervención final para puntualizar lo que tengan a bien los portavoces de los distintos grupos parlamentarios aquí presentes. Le reitero mi bienvenida a esta casa y espero que su estancia en nuestro país sea amable, fructífera y que pueda incluso tener rendimientos para el centro que usted tan dignamente representa. Tiene la palabra.

El señor **SARTS** [1] (Director of the NATO STRATCOM Center of Excellence) **(Realiza su intervención en inglés):** Señor presidente, en primer lugar, quisiera agradecerle el honor que me brindan al invitarme a comparecer ante esta Comisión. Permítame subrayar lo que voy a intentar abordar en mi exposición de hoy. Voy a hablar brevemente de lo que nosotros, en tanto que centro, hacemos. En segundo lugar, hablaré sobre la forma en la que entendemos el ciberespacio y la forma en la que el ciberespacio está cambiando, cómo está cambiando la forma en que la gente consume información y cuáles son los fenómenos que tienen que ver con este entorno. También quisiera hablar sobre cómo se puede utilizar —y de hecho, cómo se está utilizando— por parte de los actores hostiles contra las democracias, que es algo que hemos estado viendo. Y también quisiera señalar algunas de las recomendaciones que consideramos relevantes para reforzar nuestra capacidad de defender la democracia ante este tipo de riesgos.

En relación con el centro que presido, somos un centro acreditado por la OTAN, establecido por doce países, pero no formamos parte de la estructura de la OTAN, es decir, somos un organismo independiente cuya tarea consiste en investigar la guerra de la información, estudiando cada caso. Vemos cómo los terroristas utilizan la información, especialmente en el ámbito digital. Estudiamos, por ejemplo, lo que ha ocurrido en Ucrania, cómo Rusia ha empleado este entorno informativo. Y vemos también fenómenos independientes, por ejemplo, cómo se utilizan las redes sociales como armas, el aspecto digital del flujo informativo —también voy a hablar de este tema hoy— y también cómo nos basamos en este conocimiento para ofrecer herramientas a la OTAN y a sus países para que se puedan defender en este entorno. Además, ofrecemos también formación a las personas que forman parte del Gobierno y a las autoridades para que puedan operar en estas situaciones que he mencionado.

Yendo ahora al tema del ciberespacio, cuando pensamos en el ciberespacio normalmente pensamos en el *hardware*, en los ordenadores, en las redes, en las aplicaciones, en el *software*, pero lo que se nos escapa habitualmente es que también hay personas en el ciberespacio. Cuando pienso en el ciberespacio pienso, por una parte, en el *hardware* y en el *software,* pero también en las personas, en los humanos que están recibiendo información en el ciberespacio. Actualmente, la cantidad media de tiempo que pasa la gente recibiendo información en el espacio digital es del 70 al 80 %. En gran parte de los países de la Unión Europea es el ámbito principal en el que uno recibe la información, las noticias. A partir de aquí la persona va a establecer cómo percibe la realidad de lo que ha ocurrido, pero lo que ha ocurrido en este ciberespacio es que ha permitido a todo el mundo que esté presente, que pueda decir algo en este ciberespacio, lo que podría ser positivo, pero también ha permitido que cualquiera pueda tener la capacidad de ejercer una influencia en la información que se recibe. Aquellos de ustedes que forman parte de las redes sociales saben que uno comienza el día viendo cuáles son las noticias, los hilos de noticias,

[1] Este *Diario de Sesiones* refleja una interpretación al castellano no autenticada de intervenciones realizadas en inglés.

cve: DSCG-12-CM-73

pero estas noticias nos llegan a partir de personas que conocemos, que están compartiendo con nosotros estas informaciones, o, si no lo sabemos, y es lo que está ocurriendo, llega de otras fuentes, de Facebook, de Google, de Youtube… Están intentando saber qué es lo que nos gusta y ofrecernos esta información, personalizarlo, lo que por una parte es positivo, pero, si lo pensamos, también hace que la gente vea el mundo de una única manera. El impacto habitual de los medios de comunicación usuales que nos dan los dos lados de la noticia y que intentan encontrar un equilibrio está empezando a desaparecer y la gente es, cada vez en mayor medida, parte de una serie de burbujas.

Por ejemplo, está el fenómeno del terrorismo. Yo suelo citar un ejemplo muy relevante, que es cómo una persona en Letonia se convirtió en yihadista de las fuerzas del Daesh. Estaba en Letonia en una zona rural en la que no había musulmanes ni yihadistas en 100 kilómetros a la redonda, no había habido nunca, pero esa persona, este letón, era asiduo de las redes sociales y entró a formar parte de esta burbuja de la información hasta el punto que se le imbuyó la idea de que fuera a Siria a dejar su vida en esta batalla. Partía de un entorno en el que este tema no estaba en absoluto presente, así que aquí vemos lo que es la burbuja de la información.

Otro aspecto que estamos viendo en el entorno digital actual es cómo se emplean las tecnologías. Uno de los temas que quería subrayar es la robótica. Aquellos de ustedes que forman parte de medios de comunicación sociales, de redes sociales, ven que hay muchos que quieren seguirles. Ustedes son políticos y esto está bien, pero la estimación media de lo que hemos visto es que hay más de un 90 % de todas las cuentas de las redes sociales que son robots. Parecen humanos, pero en realidad son programas robotizados que se utilizan para que a usted le llegue una información determinada, para amplificar una historia determinada, para darle credibilidad y decir de alguna forma: es que su vecino de al lado se lo ha creído también.

Recientemente, hemos creado una herramienta muy sofisticada que está basada en inteligencia artificial y grandes datos que está intentando localizar estas redes robotizadas. Hemos comenzado muy recientemente y estamos examinando unas muestras muy pequeñas. Por ejemplo, Twitter, dos idiomas, ruso e inglés y, debido a nuestra zona de interés determinada, estamos examinando dos palabras código: OTAN y Letonia o Lituania. Medimos qué parte de la actividad en este sentido está robotizada. En verano nuestras conclusiones fueron que los contenidos en ruso en Twitter con las palabras OTAN, Estonia o Letonia eran hasta en un 85 % robotizados. El 85 % de este contenido estaba generado por robots. En inglés esta cantidad llegaba al 50 %. Obviamente, estamos hablando de un elemento anecdótico, porque estamos empezando a estudiar este fenómeno, pero es algo que tenemos que pensar muy seriamente. Si sus poblaciones están obteniendo la información con apariencia de que procede de una persona, de un humano —a lo mejor vemos que tenemos seguidores, imágenes de mujeres que parecen seguidoras nuestras—, como decía, aunque parece que la información procede de humanos, procede de fuentes robotizadas.

También hay un gran aumento de los grandes datos, de los *big data*. Habrán oído hablar de la historia de las elecciones en Estados Unidos. Se compraron una serie de sistemas para ofrecer información a determinadas circunscripciones y todo ello estaba basado en *big data*. Cuando nosotros, como personas, estamos en este entorno, dejamos datos detrás sobre lo que hemos hecho o dónde hemos estado. Cuando entramos en una página, normalmente hay una *cookie* que nos vincula a lo que hemos hecho; esto también pasa con nuestros teléfonos, con nuestros *smartphones*, pues solemos elegir aplicaciones gratuitas y, si las descargamos, nos preguntan por información GPS, contactos, etcétera, y esto lo utilizan para obtener datos. Las empresas que trabajan con datos están desarrollando perfiles sobre las personas: nivel de ingresos, creencias, poder adquisitivo, aficiones, viajes, y sobre esta base, estas empresas, que trabajan con grandes datos, ofrecen sus servicios para comprar anuncios y trasladárselos a aquellos a los que les podría interesar. Un ejemplo: hemos estado mirando información para ir de vacaciones a Gran Canaria, que es un destino muy importante en Letonia; a lo mejor todavía no nos hemos decidido, pero de repente nos empiezan a llegar un montón de anuncios y de información sobre Gran Canaria, dónde ir o dónde quedarse. Todo esto se basa en los *big data*, en los grandes datos, pero cada vez más se están empleando estos sistemas para influir en la opinión política. Esto ha ocurrido con Facebook y creo que es algo que va a crecer en el futuro, que va a aumentar.

Quería mencionar una última cuestión, la inteligencia artificial. Ninguna de estas cosas funcionaría, de hecho, sin la capacidad de procesar grandes segmentos de datos y dirigirlos a los elementos individuales, y esto también es el comienzo de un proceso que hemos visto que se ha producido en las redes robotizadas, que son muy fáciles de localizar. Conforme vamos viendo su desarrollo y cómo aumentan,

cve: DSCG-12-CM-73

vemos que cada vez son más sofisticadas a la hora de intentar presentarse como humanos, como personas, o de interactuar con nosotros; es decir, hay un sistema de inteligencia artificial detrás. Obviamente, no todos los trols son robotizados, también son personas. Hay un tipo de cibertroleo que a veces procede de personas, otras está robotizado o semirrobotizado —hay cuentas semirrobotizadas—. Esto es lo que hemos estado viendo. Son fenómenos que se están produciendo hoy en día, que están siendo empleados por las empresas para aumentar las ventas y también por los Gobiernos. Vamos a ver cómo podríamos utilizarlos contra una sociedad abierta y democrática. Lo que hemos descubierto en nuestras investigaciones —y hemos investigado mucho este tema, así que, si están interesados, nuestra página web contiene muchísima información sobre él— es que se examinan las vulnerabilidades; no es que se haya inventado un problema, es que es un problema que se está exacerbando, del que se están aprovechando para aumentar la división. La forma en que todas estas herramientas se están empleando tiene el fin de crear divisiones emocionales en la sociedad para que resulte muy difícil continuar con un diálogo social o político productivo; esto dificulta el diálogo. A veces se utilizan noticias falsas sin más; un ejemplo es la famosa historia que ocurrió en Alemania con la pequeña Lisa, que presuntamente fue violada por refugiados. Durante mucho tiempo esta noticia se difundió de forma considerable, pero al final se demostró que era falsa, no ocurrió, pero se utilizó para exacerbar divisiones ya existentes relativas a la política migratoria.

También se han producido toda una serie de casos interesantes en relación con el despliegue de tropas de la OTAN en los Estados bálticos. Desde que las tropas alemanas llegaron a Lituana, en el ciberespacio se produjo una especie de información, que de hecho se ofreció a los diputados del Parlamento y a los medios, diciendo que había una niña que había sido violada en grupo por soldados alemanes pero, una vez más, cuando las autoridades alemanas examinaron el caso, esta niña ni siquiera existía, es que no existía. Este tipo de casos son muy emocionales y su objetivo es dividir a la sociedad. El ciberespacio es el lugar en el que estas personas pueden desplegar este tipo de informaciones porque el elemento de la negación plausible no es fácil; es decir, no es fácil saber quien está detrás de todo esto y encontrar el espacio físico del que procede, es muy difícil rastrear quien está detrás y, por ello, resulta una forma muy útil de provocar esta negación plausible.

Hay una nueva pauta también para aquellas personas que consumen información en el espacio *online*, que es la realidad aumentada casi en tiempo real con la capacidad de alterar las imágenes, los videos o videos falsos. Ya existe una tecnología. Por ejemplo, si yo ahora estoy hablando y hay una traducción en video, hay una tecnología conforme a la cual alguien puede hacer en tiempo real que yo empiece a hacer todo tipo de gestos y traducirlo. Si ponemos todo esto en un contexto electoral, nos encontramos desde luego con un entorno muy peligroso. Está claro, creo yo, que en los temas candentes de la agenda política nacional de un lugar determinado es cuando más se emplean estas estrategias, porque es cuando resultan más efectivas. Hemos visto que estas estrategias se desarrollan en elecciones y en periodos de crisis y es fácil en una sociedad democrática. A veces no se trata solo de contar con un resultado exacto, sino de socavar la confianza en el resultado, porque pensemos en qué se basan las democracias: se basan en el hecho de que uno confía en que el resultado va a ser fruto de un acuerdo común que parte de una mayoría y si retiramos la confianza de esta ecuación, el sistema se nos viene abajo.

Para finalizar mi presentación, quisiera darles un par de sugerencias sobre lo que se podría hacer. A nivel de sociedad, creo que hemos visto que es extremadamente importante garantizar que la sociedad es capaz de resistir a estas campañas de desinformación y lo primero sería aumentar la concienciación de la sociedad. Hemos visto en algunos casos, por ejemplo, en Alemania, que la sociedad ha sido vulnerable a este tipo de efectos, pero una vez que se llegó al punto en el que el tema se debatió en gran profundidad por parte de los medios, de los políticos y de la Administración, el nivel de resiliencia se reforzó, aumentó. Es algo que hay que introducir en los sistemas educativos y también en relación con los medios de comunicación y el público en general, porque es un fenómeno que se va a quedar con nosotros durante un tiempo considerable.

En segundo lugar, y por lo que respecta a las autoridades, tenemos que aumentar la concienciación sobre la situación. Hay un elemento perturbador, y es que hay gran actividad de *malware* y se están cometiendo ataques de *phishing*, pero ¿conocemos si hay una red robotizada que en un momento dado está intentando atacar, a quién están intentando atacar, qué narrativa están empleando, qué narrativa quieren que llegue hasta nosotros con esta burbuja de la información? Esto debería ser importante para una seguridad moderna. La libertad de expresión es absolutamente importante, pero cuando los robots

cve: DSCG-12-CM-73

hablan no tienen libertad de expresión, por lo que tenemos que garantizar que no estamos permitiendo que alguien engañe a nuestros ciudadanos. También tenemos que contar con gente con la capacidad suficiente para responder en este entorno. Nosotros somos una de las entidades que son capaces de dar formación y asistencia a los Gobiernos nacionales para poder contar con estas capacidades en este entorno. Como decía, somos el producto de doce Gobiernos que han creado nuestro centro, así que el desarrollo de capacidades, tanto a nivel humano como a nivel técnico, es primordial.

Finalmente, señalaré algo que, en mi opinión, también es muy importante. Existe lo que nosotros llamamos un entendimiento de cómo se presenta la narrativa nacional. ¿Por qué funcionan estos ataques divisivos? Debido a la narrativa nacional. No estoy diciendo nada sobre España, pero en algunos casos, como en los Estados bálticos, estos temas han funcionado porque no había una narrativa nacional sólida de la sociedad como tal. Un último punto. A veces los Gobiernos no tienen la credibilidad necesaria para responder a estos fenómenos. Ha funcionado bien en algunas ocasiones en las que entidades no gubernamentales han asumido la carga de desmontar estas historias falsas, de demostrar y exponer qué es lo que está ocurriendo en realidad. De hecho, tengo un par de historias en este sentido que podría compartir con ustedes que se han producido en los Estados bálticos o nórdicos, sobre cómo han actuado estas organizaciones no gubernamentales que a veces tienen más credibilidad y una mayor capacidad para demostrar la realidad. He visto su nueva Estrategia de Seguridad Nacional en España, que está examinando muy seriamente cómo afrontar esta desinformación. Yo les diría que se unan a nuestro centro de doce naciones. Sería muy positivo, porque en este lugar podemos examinar estos nuevos fenómenos y desarrollar de forma conjunta nuestros intereses comunes y aprender lecciones comunes sobre cómo responder mejor a esta situación.

Muchas gracias.

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

Vamos a dar inicio ahora a la ronda de los portavoces, empezando por el señor Legarda, del Grupo Parlamentario Vasco.

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

Quiero agradecer la interesantísima exposición que nos ha hecho nuestro invitado y compareciente. Solo le plantearía una cuestión. A tenor de lo que nos expone, la conclusión, básicamente, es que es más fácil atacar que defenderse. En la defensa siempre se ha empleado una técnica preventiva que es la defensa disuasoria, porque todos los planteamientos defensivos en realidad son reactivos, una vez que se produce el ataque se produce la reacción, pero realmente la defensa más productiva es la disuasoria. Mi pregunta es: en este ámbito del que estamos hablando de la desinformación masificada para fragmentar la sociedad o para fragilizar la confianza en sus instituciones, ¿cabe una defensa disuasoria más allá, en su caso —que también la veo difícil—, de la defensa reactiva?

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

Doy ahora la palabra al representante de Ciudadanos, señor Salvador.

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

Míster Janis Sarts, bienvenido a esta Comisión que, como ya le ha dicho el presidente, ha celebrado otras sesiones con esta temática. Cuando terminen las comparecencias, vamos a intentar aprender de todas las aportaciones que ustedes están realizando. Comparto plenamente la intervención que ha hecho dentro del marco general de descripción de este fenómeno. En este momento estamos viendo las respuestas que se pueden dar precisamente para evitar estos fenómenos. En este sentido, ahora se está destacando que si no hay un diagnóstico que posicione un problema, difícilmente se puede buscar una solución. Es verdad que, por lo menos en España, con las elecciones de Estados Unidos y con las injerencias que pudieron existir del exterior, se empezó a ver que esto podía suceder. A partir de ahí, hemos visto fenómenos que se han producido en otros países, fuera de España y, finalmente, lo hemos terminado viendo también en Cataluña, en un proceso que está ocurriendo también en nuestro país. En este momento, España —y esta simple Comisión lo demuestra— está sensibilizada con que hay problemas que tienen que ver, en global, con la ciberseguridad, pero también con ese apartado de la falsa información y de poder generar corrientes de opinión. En ese sentido, me ha gustado mucho lo que usted ha descrito como engañar al ciudadano. Al final, lo que se crea es una percepción, un posicionamiento sobre un tema, que hace que los ciudadanos se impliquen emocionalmente de una forma concreta y que,

cve: DSCG-12-CM-73

por tanto, sus emociones deriven después en actuaciones que pueden cambiar Gobiernos, que pueden forzar una opinión pública para cambiar políticas determinadas, etcétera.

He ido apuntando, según iba hablando usted, que una de las cuestiones que considera básicas en este momento es la sensibilización sobre este problema y, al mismo tiempo que nos sensibilizamos, educar también al conjunto de la sociedad —en un mundo absolutamente globalizado y donde todos interactúan entre sí— sobre el hecho de que la desinformación también le afecta, porque a nadie le gusta que le engañen. Sobre todo, el problema que veo es el de la viralidad cuando la persona coge el engaño y empieza a extenderlo, porque entonces ya no es solo la raíz de donde partía ese engaño sino que son las propias personas las que lo están blanqueando y legitimando. Querría preguntarle si usted ve que pueden tomarse medidas gubernamentales para corregir este tipo de campañas; sobre todo me preocupa cuando sucede en los propios medios de comunicación. Hemos pasado de unos medios de comunicación en los que existían unas pautas claras: cada noticia tenía que ser contrastada, tenían que analizarse las distintas fuentes, cuando afectaba a alguien llamaban y consultaban, a que ahora mismo estemos viendo que se está mezclando todo. Con la irrupción de muchísimos medios digitales hay quien consulta y quien no, hay quien lo da ya por hecho y quien directamente desinforma. Todo eso está mezclado en este momento y quisiera preguntarle si están actuando también para ver no solamente de dónde surge, el tipo de información y qué tipo de información se hace circular, sino el uso que después hacen las personas de ello, unas seguramente engañadas y manipuladas y otras —o incluso grupos— a las que les pueda interesar en un momento determinado coger esos argumentarios para decir: lo están diciendo los medios, lo está publicando la gente y esto es verdad. Por tanto, querría preguntarle también —si no he entendido mal, desde su organismo se dedican precisamente a detectar este tipo de campañas, que normalmente para detectarlas tienen que ser muy grandes porque se tienen que referir a cosas que afecten de una manera muy importante— si considera que podría ser oportuno que, igual que están detectando este tipo de temáticas que en un momento determinado se están manipulando —por ejemplo, lo que ha dicho del video de la niña violada—, existieran portales de referencia internacional y nacional, donde se desmientan también este tipo de campañas cuando se vea que exceden la información. Creo que esto sería muy importante y que igual que existen centros de referencia a los que los ciudadanos se pueden dirigir para ver sus derechos como consumidores, se pudiera hacer lo mismo si alguien viera que está circulando un bulo muy grande. Aquí lo hacen la Policía y la Guardia Civil, a veces sus perfiles de las cuentas de Internet, pero creo que tendríamos que elevar un poquito el rango. Cuando vemos desinformaciones tan grandes, que se ven muy localizadas y que afectan a procesos muy importantes, creo que tendría que existir —por eso le pregunto a usted si lo comparte— algún tipo de publicación oficial que desmienta los bulos o avise de ese tipo de bulos, con esos robots, dando los datos y haciéndolo transparente. Se puede acusar a un Gobierno de estar manipulando o interfiriendo en un país externo y eso se puede cuestionar, pero lo que no se puede cuestionar es decir dónde están los robots, qué tipo de información están dando, en qué idioma y dónde está llegando. Por tanto, absoluta transparencia.

Para ir terminando, le quiero preguntar si cree que tendríamos que hacer cambios importantes en la legislación. En este caso me refiero a directivas europeas que actúen directamente sobre este fenómeno, que comprometan a los Estados a tener que incorporarlas y que les obligue a tener que combatirlo. Porque, claro, es muy fácil estar en un país —llámese como se llame— y decir que eso que está pasando aquí no es por nosotros o por el Gobierno, sino que se hace desde aquí pero no sabemos quién lo hace; también se puede hacer deslocalizado desde otro país y hacerlo en Asia y que desde allí estén llegando los ataques y estén organizados igual. Lo que le quiero preguntar es si se puede responsabilizar también a los Estados de que, una vez conocida la información, tengan que actuar con contundencia para desmontar esas redes que, a fin de cuentas, son redes mafiosas que están adulterando precisamente la opinión pública, repito, modificando políticas e incluso podrían cambiar el mundo. ¿Cree que se deberían endurecer las directivas europeas de aplicación obligatoria por parte de los Estados y establecer penas en consecuencia por el daño que se pueda hacer? Estamos hablando de poder cambiar la opinión pública de todo un país y darle la vuelta mediante la manipulación, por lo que le pregunto si usted considera que tendría que haber una serie de penas importantes para las personas que participen activamente en ese fenómeno.

Muchas gracias.

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

Tiene la palabra el señor Alonso.

cve: DSCG-12-CM-73

El señor **ALONSO CONTORNÉ:** Muchas gracias, señor presidente.

Muchas gracias, señor Janis Sarts. Su comparecencia ha sido muy interesante, pero me voy a detener en su resumen final porque creo que nos ayudará mucho. Nosotros entendemos que hay que separar lo que es la ciberseguridad de la desinformación; no sé si el compareciente está de acuerdo o no. Nuestro grupo, Unidos Podemos-En Comú Podem-En Marea, tiene clarísimo que estará al lado de todo el mundo para defender y trabajar conjuntamente por la ciberseguridad, pero en el tema de la desinformación tenemos dudas. ¿Por qué? Evidentemente, estamos en contra de la desinformación, pero lo que no tenemos claro es dónde marcar esa raya, quién determina esa raya entre lo que es desinformación y lo que no es desinformación. ¿Quién lo determina? ¿El señor Eduardo Inda, el señor Vincent Sanchis, la señora Tarribas, el señor Margallo o yo mismo? No lo sé, por tanto, creo que es importante saber dónde empieza y dónde acaba la desinformación, cuestión que creo que en su resumen final nos ha explicado.

Hace unas semanas, a nuestro entender, tuvimos un momento de desinformación. Me estoy refiriendo a la teoría del «pato», cuando el señor Hernando —yo no sabía de qué Hernando hablábamos— nos trajo a una ponente, la señora Milosevich, que, con todo el respeto, nos vino a decir que estábamos en guerra de desinformación con Rusia. Mi pregunta es: ¿Usted piensa exactamente igual? Yo, que vengo de Cataluña, pregunto: ¿Estamos en guerra o falta implementarla? Es importante saberlo, porque para nosotros es una cuestión preocupante. Estamos hablando de un país soberano, de un país respetuoso como cualquier otro, y leímos una carta del embajador quejándose de esto, sin querer hablar de Podemos porque el oro de Moscú antes lo teníamos los comunistas y ahora parece que lo tienen los de Podemos. Sin querer hablar de esa tontería, que no queda ni puede quedar demostrada en ningún caso, le pregunto si tiene el mismo criterio. También encontramos unas manifestaciones del Instituto Nacional de Criptología donde nos dice que no hay ningún rastro de ciberataques a España. Eso se contradice con lo que se decía en la teoría del pato a la naranja, porque, si este instituto dice que no hay rastro, estamos dando por seguro que hay una guerra de desinformación con Rusia o estamos apostando por que eso es así. Nos hablan de granjas de bots y de trols. Es verdad, existen y existirán posiblemente en muchos lugares y como nosotros tenemos experiencia —yo soy catalán y en la Costa Brava teníamos una cosa que se llamaba Radio Liberty; ahora son de otra forma esas actuaciones—, también tenemos esas granjas de bots y esas granjas de trols para actuar lógicamente contra un supuesto enemigo, es importante saberlo porque así sabremos cómo actuar al respecto y seremos más eficientes a la hora de contrarrestar esa situación.

Hay una cosa —y aquí me meto con el señor presidente, con todo el respeto, por supuesto—, usted, que tiene mucha experiencia en el tema de defensa y lógicamente en el tema de defensa en Letonia, yo recuerdo —se ha mezclado demasiado y es importante aclarar que no tiene nada que ver— unas declaraciones en La Vanguardia, que para mí es un periódico serio, no una granja de bots, decía en un titular: Letonia —estamos hablando del 13 de septiembre de 2013— abre la puerta a reconocer a una Cataluña independiente. Esta información decía eso y aparecían unas manifestaciones del primer ministro, etcétera. Usted ha estado en el Ministerio de Defensa de Letonia y quizá no tiene nada que ver —espero que sea así—, pero el señor Margallo nos vino a decir no hace mucho —unas declaraciones que creo que le escuché personalmente— que debíamos algunos favores en algunos lugares sobre el tema de Cataluña. No hace falta ser un trol ni un robot que no tiene derecho a la libertad de expresión, pero todos recordamos que en 2016 llegamos a un acuerdo por el cual tenemos carros de combate en Letonia en la frontera con Rusia. Supongo que usted lo conoce. Además, da la casualidad de que por primera vez se buscó una estratagema para que eso no pasara por el Congreso.

Ahora sí que me referiré al tema que usted ha mencionado al final y que comparto totalmente, y es si estamos diferenciando entre lo que es desinformación y lo que es ciberseguridad. Concienciación de la sociedad, correcto. Usted hacía una reflexión que creo que es fundamental. ¿Por qué funcionan estas desinformaciones? Decía que porque no existe una narrativa nacional o porque sí existe una narrativa nacional, como en el caso de los soberanistas de la DUI, aunque no todos los soberanistas son de la DUI. ¿Por qué funciona tan bien? Porque hay gobiernos que no tienen credibilidad y ese es un problema que, desgraciadamente, tenemos también en España. Dicho esto, la mejor solución que usted planteaba y que también han planteado otros ponentes es el periodismo. El periodismo es la mejor forma de combatir la desinformación; lógicamente un periodismo independiente, pero sobre todo riguroso y honesto.

Muchas gracias.

cve: DSCG-12-CM-73

El señor **PRESIDENTE:** No sé si el padre del «pato» quiere contestar. **(El señor Hernando Vera: No).** Yo sí que contestaré —supongo que dentro del Reglamento—, puesto que he sido directa y personalmente aludido, pero lo haré después de que haya hablado el señor Sarts, lo mismo que puede hacer el señor Hernando, que es el portavoz del Grupo Parlamentario Socialista al que usted se refería. **(El señor Hernando Vera: Como decía mi madre, demasiado aprecio).** Dejamos al «pato».

El señor Raffo tiene la palabra.

El señor **RAFFO CAMARILLO:** Muchas gracias, presidente.

El problema del «pato» es que, cuando existe, existe por sí mismo. Es puro materialismo. Los hechos y las cosas existen independientemente de nuestra propia existencia. Otra cosa es que pretendamos, idealizando la realidad a nuestra conveniencia, intentar negarla, pero eso se aleja bastante del materialismo dialéctico, que es un buen instrumento de análisis y enfoque de la realidad, más allá de lo que puedan pensar los idealistas puros. Yo me considero dentro de ese grupo desde el punto de vista de un enfoque científico de los hechos y de los acontecimientos.

Ha mencionado el asunto de la niña. Era ruso-alemana y lo que se pretendía precisamente era una reacción xenófoba en la población alemana y que también reaccionara la población rusa hacia el pueblo alemán. Ahí hay un gran secreto, que es este. Esa información no solo pretende producir desestabilización y la falta de cohesión social en lo que se podía identificar como un adversario, sino que está hecho también para consumo interno, para generar la idea de que una potencia se encuentra en sus valores por encima de otras que se intentan degradar a través de una serie de razonamientos y argumentos con noticias falsas o con la manipulación de los hechos. Tampoco se puede negar que haya una tensión. Una de las dudas que tengo es que precisamente España no es de los países que han sido más contundentes o beligerantes dentro de la órbita de la Unión Europea con Rusia, pero no dejamos de formar parte de la Unión Europea, esa es la realidad. Con ello no estoy dando a entender ni estoy concluyendo que el Gobierno ruso esté detrás de esto, pero lo que sí es verdad es que en una avenida en Moscú hay un centro denominado granja de trols, la casa de las mentiras, que viene hasta con el nombre en algunos medios de comunicación y de la que hay fotografías; tiene varias plantas, donde funcionan distintos especialistas. Mi pregunta, en primer lugar, sería: ¿Existe esa granja? **(El señor presidente: En San Petersburgo)** No, la que yo leo aquí dice que es en Moscú. Yo sé que en San Petersburgo hay una agencia privada que vende su producto al sector privado, a Gobiernos, etcétera, a nivel global, no es solo que funcione cuando interesa al sector público, aunque sea con un interés legítimo y desde la bondad más absoluta.

Siguiendo con lo del «pato». Como estamos hablando de ciberdefensa y de ciberseguridad y no de ciberataque, nadie está planteando que España se organice con otros países de la Unión Europea para copiar el modelo y, a partir de ahí, identificando que hay una agresión, realizar otra y entrar en esa escalada. Lo que sí tendremos que demostrar es que somos capaces de defendernos de estas agresiones. Creo que ha planteado un elemento muy importante que ya abordamos en la reunión anterior —era el motivo más importante o más destacado de lo que iba a ser mi intervención—, que es la potenciación de la alianza y la asociación de más países de la Unión Europea en este centro, que contaría también con la colaboración española.

Me gustaría terminar con dos cuestiones, para ser lo más breve posible. En primer lugar, quisiera decir que la expresión bomba informativa proviene de los profesionales de los medios de comunicación y también la manejamos en el ámbito político. De hecho, son bombas informativas porque lo que pretenden es desgastar a una sociedad en el plano psicológico, en las relaciones sociales, etcétera. Son auténticas bombas informativas. He visto a través de WhatsApp, por unas conexiones que no voy a mencionar, tanques circulando por Barcelona; barcos de la Armada de Barcelona anclados en el puerto de Barcelona; fotografías de tanquetas, que no eran ni del Ejército español, que, aparentemente, decían que eran en Barcelona… Eso era desinformación. Esto es real.

Yo aprendí mucho de lo relacionado con la mentira y la verdad leyendo a Hannah Arendt —un clásico—, pero también había un filósofo e historiador de la ciencia que se llamaba Alexandre Koyré, un ruso que se exilió a Estados Unidos, en cuyo libro titulado *La función política de la mentira moderna* o r*eflexiones sobre la mentira* decía que el progreso técnico en la comunicación de masas era la innovación poderosa de todos los regímenes totalitarios y denunciaba que la usurpación de las nuevas tecnologías —en el año 1943— por sectarios sin escrúpulos ponen al servicio de la mentira todo lo necesario e implica la destrucción del espacio público. Eso es lo que se pretende.

Muchas gracias por su intervención y por la información que nos ha facilitado.

cve: DSCG-12-CM-73

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

Tiene la palabra el portavoz del Grupo Popular, señor Aznar.

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

En primer lugar, quisiera agradecerle su intervención, señor Sarts, que viene a complementar otras suyas a las que hemos podido tener acceso. Nos parece realmente interesante todo lo que hoy nos ha trasladado, como han dicho el resto de mis compañeros portavoces.

La impresión que vamos teniendo en esta Comisión a medida que vamos escuchando a los distintos intervinientes es que hoy día se puede constatar que se están produciendo todos estos ataques de los que se habla, más allá de que algunos crean que son cuestiones de «conspiranoicos», utilizando herramientas o elementos que ya se utilizaron en la Guerra Fría pero implementados con las nuevas tecnologías. Parece que esta conjunción de estrategias y de herramientas que se están utilizando cada día es más patente. Por otra parte, hay una serie de hechos, de alguna forma probados, que son los ataques que se producen en distintos países y en distintos años a la hora de celebrarse procesos electorales. Por recordar alguno, sin ánimo de ser exhaustivo, tenemos los del año 2009 en Estonia: en 2014, también coincidiendo con las elecciones, en Ucrania; en 2015, en Alemania; en 2016, en Montenegro; en 2017, en Noruega; también en los Países Bajos, sin hablar ya de los más recientes y cercanos como pueden ser en las elecciones francesas, y está en la mente de todos la influencia que se intentó en las elecciones americanas. Si todo esto es real, y parece que se constata que todo esto se produce, me gustaría saber su opinión sobre quién está detrás de todo ello, más allá de lo que usted ya nos ha dicho de que es muy difícil hacer una constatación real y física de dónde está y de dónde sale la decisión para que todas esas cuestiones se lleven a efecto. Es verdad que los Gobiernos están reaccionando y que en cada país se están utilizando medios para hacer frente a estas circunstancias. Me gustaría saber si, en su opinión, hay realmente una coordinación, al menos entre los países más cercanos a nosotros, que son los países OTAN, o habría que implementar de alguna forma esta coordinación, porque lo que es una realidad es que un país por sí solo es muy difícil que pueda afrontar en el futuro esto que se está produciendo. Yo creo que esto es —no habría que tener temor a decirlo— una guerra; en realidad estamos asistiendo a una guerra y en algunos países —creo que usted en alguna de sus conferencias lo ha mencionado— se está intentado actuar y haciendo que la población civil reaccione, utilizando, en el mejor de los sentidos, a la población civil para hacer frente a los ataques. Me refiero a la actuación en países de su entorno más cercano, como Letonia o Lituania, de los llamados elfos que, en definitiva, son ciudadanos corrientes a los que se pide que colaboren activamente para frenar estas desinformaciones, estos ataques.

También me gustaría saber su opinión sobre si realmente se está produciendo esta situación de guerra en el ciberespacio —aunque suene muy fuerte— y si la utilización, en el mejor de los sentidos, de la población civil para colaborar con los Gobiernos es de alguna forma útil. Es verdad que hay que sensibilizar a la sociedad, y en esto tenemos que hacer un esfuerzo todos los Gobiernos; hay que trabajar con los medios de comunicación y fomentar, de alguna forma, que la investigación seria, la investigación razonable desde los medios de comunicación más competentes sea también una forma de colaborar, sobre todo en lo que se refiere a la desinformación. Los países estamos tomando conciencia y adoptando algunas medidas. Concretamente en España, la vicepresidenta del Gobierno anunciaba ayer la puesta en marcha en los próximos meses de un mando único en materia de ciberseguridad, lo que quiere decir que en los distintos países se están haciendo cosas concretas. Me gustaría saber, al igual que el portavoz de Ciudadanos, si tiene usted alguna sugerencia en materia de cambios legislativos que desde la Unión Europea haya que promover.

Por último, una cuestión más concreta en relación con su centro. Usted nos hace una invitación, que estoy seguro que sería muy provechosa, para que España se sume a esos once países, pero me gustaría pedirle que nos hiciese resumidamente una comparación entre el centro que usted representa y el que existe en Tallin, ya que de alguna forma están haciendo labores similares. Creo que más allá de que a algunos les moleste que se cite a países concretos, esto se está produciendo y me gustaría que usted nos dijese de dónde proceden, en su opinión, estos ataques. Una vez más quiero agradecerle su comparecencia hoy aquí ya que, sin duda alguna, nos va a ser de mucha utilidad.

Muchas gracias.

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

Antes de dar la palabra al señor Sarts, para ir despejando alguna de las cuestiones que no se refieren directamente a él, voy a intentar contestar al señor Alonso, agradeciéndole la forma en que lo ha planteado.

cve: DSCG-12-CM-73

En primer lugar, materialismo dialéctico, los hechos. Es verdad que en 2013 había en parte de la sociedad catalana una cierta tentación de emular la vía báltica y que había sectores —fundamentalmente privados— en los países bálticos que tenían una cierta simpatía hacia el proceso independentista catalán y hacia los procesos independentistas en general. Como sabe mejor que yo el señor Sarts, los países bálticos accedieron a la independencia, por cierto, no ejercitando el derecho de autodeterminación que estaba previsto en la Unión Soviética, denunciando el Pacto Ribbentrop-Mólotov. Primer hecho. El segundo hecho es que hubo un intento por una parte de la sociedad catalana de influir en los países bálticos en los puntos que consideraban de más debilidad, el escalón más débil de la cadena, si puedo seguir utilizando terminología marxista.

Segunda cuestión. Nosotros somos socios de los países bálticos en Naciones Unidas, tuvimos el voto de los tres en el Consejo de Seguridad; somos socios en la Alianza Atlántica y también en la Unión Europea. Es regla general de cualquier sociedad que antes de cualquier reunión un socio ponga encima de la mesa cuáles son sus intereses y sus prioridades. La prioridad del Gobierno español, al que yo representaba, era mantener la unidad de España y la vigencia de la Constitución, como es obvio. La cuestión que preocupaba a los países bálticos era Rusia. Es absolutamente verdad que nosotros, cumpliendo con nuestro deber de socios leales y fiables, hemos colaborado en esfuerzo militar, no solo en tierra sino también en aire, y hemos votado religiosamente con los aliados de la Unión Europea en cuanto se ha hablado de sanciones para Rusia después del referéndum sobre autodeterminación de Crimea, que fue declarado nulo por Naciones Unidas. En justa contrapartida a esos esfuerzos —favores, como usted dice—, que son los que corresponden a un socio leal, hemos planteado siempre que para nosotros, insisto, la defensa de la Constitución era prioritaria y que no entenderíamos ni entenderemos que un Gobierno socio nuestro haga un ataque frontal a la integridad territorial. Argumento fácil de probar porque está en tres resoluciones de la Asamblea General de Naciones Unidas que exhortan a todos los países de la organización, a los 193, a no adoptar ninguna medida que pueda suponer aliento o apoyo a cualquier maniobra secesionista unilateral. Esto es así y la última la redacté personalmente cuando presidimos el Consejo de Seguridad.

Me preguntaron en Cortes si era verdad que yo, como ministro, estaba intentando exponer las razones de España en contraposición con las razones de un proceso secesionista hecho por otras organizaciones —últimamente desde la misma Generalitat, cuya legitimidad viene de la Constitución y del Estatuto— y dije que sí, que era verdad, que lo estaba haciendo, no solo en los países bálticos sino en cualquier otro sitio donde pudiese ver una fisura. Y terminé diciendo que no había sido nombrado ministro de Asuntos Exteriores para dinamitar la unidad de España. Esto es todo lo que tenía que explicar y si el señor Hernando no quiere hacer ningún comentario terminamos con las alusiones personales.

Señor Sarts, tiene la palabra.

El señor **SARTS** (Director of the NATO STRATCOM center of excellence): Quiero darles las gracias por sus más que interesantes preguntas. Voy a intentar responder a todas ellas punto por punto. Obviamente, la defensa únicamente no nos da la capacidad de solventar esta situación. Los datos muestran que una vez que esas noticias falsas altamente emotivas están ahí, resulta muy difícil, a la hora de verificar hechos, alcanzar la misma actitud. Sobre las alegaciones falsas sobre Clinton y cómo se compartieron en las redes sociales hay que decir que se compartieron más de un millón de veces, por lo que establecer cuál es la verdad sobre esta misma historia o alegación —que llegó a 10 000 noticias compartidas— es uno de los problemas que abordamos aquí; la predisposición de las personas para creer o no lo que quieran o no creer. Por tanto, para abordar este tema hay que tener en cuenta, en primer lugar, que la gente que está precondicionada está muy influida por estas historias tan altamente emocionales. Además, tenemos que ser los primeros en el entorno informativo y decir: esta es la realidad. Las opiniones pueden variar pero los hechos son los hechos, es decir, si hay un tanque en Ucrania Oriental y es un tanque ruso, es que es un tanque ruso, no se le puede dar más vueltas. Esto es algo que se está intentando hacer, esta forma de dar vueltas a los hechos. Hay veces que lo podemos hacer, podemos emplear la tecnología para garantizar qué es lo que se está planteando y presentar los hechos de la historia.

Segundo elemento. No es que siempre tengamos que estar destinados a responder sin más. Podemos entender la forma en cómo se está intentando socavar y utilizar estas vulnerabilidades. Podemos construir sistemas sobre cómo responder. Para la mayoría de los Gobiernos, el área clave en la que hay que defenderse es en las elecciones. No se defienden las elecciones reaccionando, tenemos que establecer

cve: DSCG-12-CM-73

un sistema conforme al cual garanticemos que las elecciones son libres y que no hay influencias, especialmente del exterior. Esto me lleva a uno de los otros puntos que se han suscitado, el de la legislación, la reglamentación. Hay que se muy prudentes, lo que estamos intentando es encontrar un equilibrio muy delicado entre, por una parte, garantizar la libertad de expresión y, por otra, garantizar que la desinformación no está influyendo en la opinión pública. Hay que encontrar ese equilibrio, y es delicado. Podemos hablar sobre cuáles son los parámetros, pero un asunto clave en este sentido es que cuando las naciones van a celebrar elecciones hay toda una serie de normas, de leyes que entran en juego. Si se financia, hay que ser transparente; si se hace publicidad, hay que hacerla de una determinada manera; o por ejemplo no se puede hacer campaña política uno o dos días antes de las elecciones. Hay toda una serie de normas. ¿Todo esto se cumple en los medios de comunicación social? Por ejemplo, si alguien compra una *botnet* y se presenta como el vecino de al lado, ¿cómo establecemos la relación? ¿Eso es correcto, se puede hacer? Hay ámbito para regular. Podemos analizar Twitter mediante una serie de sistemas que son abiertos pero, por ejemplo, Facebook, no, salvo que estén dispuestos a compartir con nosotros qué es lo que está ocurriendo, si no, no lo podemos saber y entonces tendría que entrar en juego la inteligencia para examinarlo. ¿Es correcto que alguien que no forma parte del sistema haya comprado toda una campaña y esté difundiendo un mensaje electoral determinado? En mi opinión, hay ámbito para el debate sobre la legislación y la regulación y no basta con una regulación nacional —esto también quería decirlo— porque podemos desplegar fácilmente nuestras operaciones en Letonia o en España pero hay que ir a un nivel superior.

También es importante desarrollar diálogo con las empresas que se dedican a la tecnología porque ellos tienen una serie de claves, de algoritmos, que podrían solventar el problema. Así que, aparte del debate sobre la legislación, es necesario el diálogo con las grandes compañías tecnológicas para que ellas también puedan realizar una aportación positiva para solventar el problema. En vez de evitarlas y que al final veamos que alguien externo ha comprado una serie de campañas, hay que detectar estas campañas. Hay dos elementos que hay que examinar aquí. Nuestra tarea, en tanto que centro, es entender el problema, profundizar en el conocimiento y sobre esta base ayudar a las naciones a desarrollar metodologías y ofrecer formación para el desarrollo de capacidades. Nosotros no somos *per se* capaces de supervisar todo el espectro, pero en algunas ocasiones, por ejemplo cuando vemos *botnets* comparativamente pequeños, cuando vemos lo que están haciendo los elfos, también vemos otras cosas. Por ejemplo, Cataluña fue uno de los puntos álgidos de la comunicación de un *botnet*. Al mismo tiempo, el tipo de mensajes que se están difundiendo por estas redes también nos dan una idea sobre quién podría ser la parte interesada. Algunos anuncian mensajes políticos y luego lo que comunican son anuncios o anuncios para adultos, pero algunos de ellos se limitan a un mensaje político, y además un mensaje político determinado. Aquí podemos establecer una imagen más limitada. Nosotros no somos una agencia de inteligencia, no vamos examinando las direcciones de IP una por una, pero sí puedo obtener una imagen determinada y advertir a sus autoridades nacionales que examinen con mayor profundidad una serie de temas.

Tema de Rusia. Hay una pauta que hemos visto. En alguno de los casos se ha demostrado amplia evidencia en el sentido de que el Gobierno ha estado involucrado, casos como Ucrania o Alemania —el caso que mencionábamos, que es muy obvio—, y también se está dando una emergencia de noticias de los Estados Unidos donde yo creo que estuvo implicado el Gobierno, porque no creo que esta operación hubiera podido ser realizada sin el consentimiento de las instancias más altas del Gobierno. Es mi opinión personal. Lo que se puede decir es que la mayoría de estas pistas sobre direcciones de IP nos llevan a territorio ruso. Por ejemplo, circuló una carta falsa del ministro de Defensa sueco a una empresa en 2015 sobre una supuesta entrega de armas a Ucrania que no era real pero causó un caos político bastante considerable en Suecia porque habría sido algo inaceptable, un gran escándalo. La dirección de IP nos llevaba a San Petersburgo. También hubo otro caso interesante en 2014 en Estados Unidos relacionado con una planta química. En este caso, en 2014, había toda una serie de tuits que nos llevaban a vídeos y noticias de la CNN sobre un accidente en una planta química en Columbia, en Luisiana, y luego este accidente no se había producido. También había un vídeo del Daesh que decía que eran responsables de ello y una vez más aquí los expertos cibernéticos examinaron las direcciones de IP y vieron que estaban en territorio ruso. Yo no puedo decir quién estaba dando estas informaciones, pero está claro que hay una línea factual en estos casos concretos.

Sobre los medios de comunicación ha habido muchas preguntas. Un tema que creo que tenemos que entender en relación con los medios de comunicación es la forma en la que fluye la información en una

cve: DSCG-12-CM-73

sociedad moderna. Esto ha cambiado de forma muy importante. Solía ser más o menos jerárquico, es decir, los líderes de opinión de una sociedad hablaban, los medios escuchaban y lo trasladaban a la población. Era como un flujo vertical de información con diferentes opiniones y con una serie de normas periodísticas a la hora de presentar la historia desde los diferentes ángulos en juego. Pero todo ello ha cambiado en la mayoría de nuestras sociedades, ha cambiado muchísimo. Ahora son los medios de comunicación o cualquier persona los que pueden comunicarse con otros. Ciertas redes, que algunos llaman medios de comunicación digitales, se parecen a los medios de comunicación porque tienen una serie de normas éticas o de verificación de los hechos, pero otras son sensacionalistas. Hay una forma de ganar dinero haciendo clic en una historia. En Letonia, por ejemplo, ocurrió el siguiente caso: un niño desapareció y posteriormente se supo que se había perdido en los bosques y que había fallecido, lo cual fue una tragedia terrible. Luego se empezaron a reenviar historias en las que se contaba que había otro niño perdido y esto creó una atmósfera muy emotiva; se empezó a compartir esta noticia, pero al final era falsa. Por tanto, aquí hay un modelo de negocio. Yo no las llamaría medios de comunicación desde luego, pero están teniendo un impacto, y ese es el problema porque se presentan como fuente creíble. Por tanto, para que los medios de comunicación puedan responder a este sensacionalismo tiene que haber políticas gubernamentales que alienten un buen periodismo que dé información objetiva, presentando todos los lados y las diferentes opiniones de la historia, y que corten los incentivos financieros a las que están siendo especialmente sensacionalistas y que de forma intencionada están transmitiendo historias falsas de gran carga emocional para ganar dinero, sin más.

También hay negocios basados en el clic —se transfiere el tráfico de información a una entidad y se obtiene el dinero a partir de Google— y se dedican a temas sensacionalistas: difunden noticias sobre coches, mujeres, bromas. Se ha dado el caso de que uno de estos negocios basados en el clic fue adquirido no por un partido político sino por una entidad. La red, que era muy amplia —más que cualquier otro medio de comunicación en aquel país—, comenzó a introducir mensajes políticos en el momento específico en que se estaba debatiendo el presupuesto y esto tuvo un impacto muy importante en el debate nacional y, de hecho, en pocas semanas ese impacto creció. Un periodista investigó y se dio cuenta de que alguien había comprado esta red; examinó toda la historia y dijo lo que había ocurrido, quién lo había comprado y aquí se acabó la historia. Una vez más nos encontramos con un caso que ejemplifica tanto la naturaleza horizontal del impacto que estas redes pueden tener en la sociedad por no realizar ninguna verificación y no tener ningún equilibrio, así como la importancia de la sociedad civil a la hora de responder a este problema dándole o no credibilidad.

Otra cuestión que quería comentarles es que es muy peliagudo que el Gobierno sea el que tenga que decir siempre si esto es verdad o no; tendría que ser alguien delegado por la sociedad, alguien absolutamente independiente —con autoridad, con credibilidad y sin connotaciones políticas— el que dijera que algo es falso, lo que sería clave y la mejor solución, porque si el Gobierno es el que se manifiesta se infravaloraría su opinión.

Por último, me referiré al centro de Tallin y al nuestro. Cooperamos estrechamente: ellos examinan el aspecto técnico de la ciberseguridad y nosotros examinamos el contenido informativo, cómo se difunde la información, el aspecto cognitivo, así que creo que nos relacionamos muy bien, cooperamos y no duplicamos nuestras tareas, porque es un ámbito en el que hay un trabajo ingente.

El señor **PRESIDENTE:** Muchísimas gracias.

Vamos a empezar la segunda ronda. ¿El señor Legarda quiere intervenir? **(Pausa).** ¿El señor Salvador quiere intervenir? **(Pausa).**

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

Compartimos plenamente su intervención porque esto va de eso, pero lo que no entendemos mucho es cómo puede haber gente que en pleno siglo XXI y en la era en la que estamos se pueda sorprender cuando se habla de estos conceptos. Hace no muchos años estábamos hablando de guerra fría en la que había bloques, cada uno con sus intereses y que querían una visión del mundo totalmente diferente, lo que provocó un choque, algo que todos lo hemos concebido y visto en el cine y en otros lugares. Antes se llamaba Guerra Fría, pero a partir de la desaparición de esta Guerra Fría con la caída del muro de Berlín, se generaron los cuarenta conflictos olvidados, donde explota medio mundo porque ya no eran los tuyos y los míos, ya no se trataba de tú no te metas en los míos y yo no me meto en los tuyos sino que cada uno iba por libre y a partir de ese momento hemos visto también los líos que tenemos y que hay que resolver en muchos conflictos regionales.

cve: DSCG-12-CM-73

Hace mucho tiempo se empezó a hablar precisamente de un país que no se está mencionando nada actualmente, y tampoco hace falta, que era China, que estaba actuando en prepararse para este tipo de terreno de una manera muy importante y haciendo que muchísima gente recibiera formación y organizándola militarmente para actuar en un momento determinado en estos campos; no digo si en un sentido bueno o malo, pero eso está ahí.

Esta Comisión, que es una Comisión sobre ciberseguridad, evidentemente está teniendo distintos comparecientes y cada uno de ellos está hablando de distintos aspectos de la ciberseguridad. Hoy comparece usted para hablar de uno en concreto y otros para hablar de otros temas; lo digo para defender al presidente porque parece que ahora nos ha dado por la desinformación. La actualidad es esta y el Partido Socialista pidió que se le diera un tratamiento a estas cosas que estaban surgiendo en la información, por ese motivo estamos dedicándonos un poquito más a esto de la desinformación que es, por otra parte, absolutamente importante. Esto no va de un mundo de buenos o malos. Si a los que hacen la desinformación yo los considero de los míos, entiendo que está bien y tengo que defenderlos si alguien los ataca, sea Rusia o Venezuela, pero si lo hacen otros, yo sería el que atacase diciendo que eso está mal porque lo están haciendo otros países. Lo que aquí estamos analizando son las prácticas, si son buenas o malas, en qué pueden incidir y evitar que se hagan. Otra cosa es que estemos hablando del hecho objetivo de quién las está realizando y en este momento han pillado con el carrito de los helados en Rusia a Rusia o también es el caso de Venezuela. Por tanto, si alguien se sorprende de eso, que se lo revise porque me parece que en ese sentido está desenfocando el concepto de intentar evitar que esto pueda pasar. Por ejemplo, existen las asociaciones de consumidores para garantizar que no haya publicidad engañosa y que los ciudadanos no sean estafados en las cosas que tienen que consumir; esas asociaciones de consumidores actúan, emiten informes, algunos son preceptivos, tienen consecuencias y algunos llevan sanciones. ¿Qué es lo que pretendemos? Que el usuario pueda recibir todas las campañas de información que quiera pero, al mismo tiempo, que no se le venda, falseando, un producto.

Hay que ver también el tema de la privacidad porque usted ha planteado aquí dos elementos muy importantes que se utilizan hoy como herramienta: el *big data* y la inteligencia artificial, y es verdad que nos pueden conocer a nosotros mejor nosotros mismos pero, vamos a ser sinceros, ¿la sociedad quiere que se la conozca mejor que sí misma? ¿Hemos acabado ya con la privacidad del ser humano? Es decir, ¿cuando una persona navega por la red, no tiene derecho a navegar por donde crea que quiere hacerlo mientras no haga algo ilícito? ¿Tienen que tener determinadas empresas un patrón determinado que pueden utilizar para bien o para mal con esa persona en un momento determinado? Por tanto, estamos entramos entrando en un terreno al que es necesario dar normativa, elaborar una legislación y ponernos de acuerdo en cómo preservar la libertad individual al mismo tiempo que avanza la sociedad para proporcionarnos cosas que sean buenas. Si desenfocamos el tema, si lo hacemos los míos y los otros, no estaríamos yendo a la raíz y difícilmente conseguiremos información importante para progresar.

Todo el mundo defiende la formación, y la formación para recibir buena información, como un elemento que puede garantizar la libertad de los ciudadanos. Es decir, si los ciudadanos están formados será mucho más fácil que no se les pueda engañar, sabrán cómo se tienen que defender o cómo pueden acceder a una información que sea veraz. Cuando los ciudadanos están desinformados y en sociedades que no tienen formación adecuada, evidentemente son mucho más vulnerables. Por eso, todos los que creemos y defendemos las sociedades modernas decimos que el valor principal, no solo para la economía y para competir, está en la formación pero para tener ciudadanos libres e iguales. Aquí estamos hablando, y usted nos ha venido a hablar, de desinformación y de cómo esas campañas organizadas pueden incidir en la sociedad y que además eso se puede hacer de una manera que aparenta ser lo que no es. Estoy de acuerdo con usted cuando ha dicho que tienen que ser organismos independientes los que auditen en este sentido y desarrollen la información que tengan que hacer pero, aquí también se ha dicho, hay hechos y estos hechos sí se pueden describir en todo momento.

Aquí estamos hablando ahora mismo sobre actuaciones políticas para cambiar opiniones públicas sobre conflictos muy sensibles. Llevamos muchísimos años hablando de la unidad de España y de la importancia de nuestras comunidades autónomas y de cómo tener todo el encaje para que ahora venga alguien desde fuera de España a desinformar al conjunto de la gente y a lo mejor de manera decisiva para liárnosla más y tratar de romper la unidad de este país. Por tanto, estamos hablando de un tema muy serio. Hace no mucho tiempo los militares también empezaron a afrontar el tema de la información económica, porque hoy también se puede hundir a un país o se puede hacer que un país tenga problemas o se puede hacer que determinados fondos de inversión de repente multipliquen sus beneficios y haya

cve: DSCG-12-CM-73

sociedades que sean más pobres. Todo esto está viniendo de la mano de la tecnología y puede tener un bueno uso o puede tener un mal uso. Nosotros, como gobernantes, tenemos que defender un bueno uso de todo esto y, sobre todo, que no se pueda manipular ni engañar a nadie y que tengamos defensas para garantizarnos una sociedad libre de ciudadanos libres e iguales. Por tanto, le quiero animar en su trabajo, en este apostolado que también está haciendo hoy en España para que siga desarrollándose. Hay que implicar una red en toda la Unión Europea que esté conectada para trabajar muy sincronizadamente: se diagnostica, se detecta, se informa y se actúa. Hay que ver cuáles son los niveles en los que se puede actuar, pero, repito, desde un pensamiento mucho más profundo de los efectos del *big data*, de la inteligencia artificial, de la manipulación de la desinformación y, sobre todo, de preservar la libertad de los ciudadanos. Así pues, le animo a que siga con esta cruzada de apostolado, porque creo que es importante.

Deseo invitar a mis compañeros de Comisión de distintas ideologías y de distintos partidos políticos a que no veamos esto como los nuestros o los otros, porque si lo vemos así difícilmente nos pondremos de acuerdo sobre qué puede ser ético o no ético, bueno o malo, que es lo que tenemos que hacer para que ningún país pueda lanzar una intromisión en cosas que un día nos pueden venir bien pero otro día nos pueden venir mal.

Le agradezco de nuevo su intervención. Muchas gracias.

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

Señor Alonso.

El señor **ALONSO CANTORNÉ:** Muchas gracias, señor presidente.

También deseo agradecerle su explicación, porque creo que es necesaria y oportuna. Yo la había escuchado en otra ocasión, pero creo que es importante que se vayan clarificando y que se vayan explicando las cosas tal como son, no con diferentes interpretaciones.

Yo le recordaría —por alusiones indirectas— al amigo Luis, al compañero de Ciudadanos, que si alguien en estos momentos —es que yo vengo de Cataluña, yo soy catalán— está hablando de bloques o está hablando de tuyos y míos no somos precisamente nosotros; son otros los que están hablando de tuyos y míos. Eso es un error y lo estamos padeciendo desgraciadamente. A lo mejor eso no ayuda en voto, pero sí ayuda en sentido común, y precisamente ayuda a tener una sociedad reconciliada, que es lo que nosotros estamos pidiendo.

El día 12 de este mes se publicaba en un periódico, en el que, por cierto, yo he trabajado durante años y en el que desgraciadamente se está despidiendo a veintiséis trabajadores —lo que también influye en que luego tengamos los medios de comunicación que tenemos, que son muy débiles; luego hablaremos de lo que usted ha hablado al final, que también me ha parecido muy interesante—, que un exejecutivo —que era el vicepresidente— de Facebook asegura que las redes sociales están destrozando la sociedad. El nombre de dicho exejecutivo es un poco complicado porque es hindú y por eso no lo voy a leer, pero se afirmaba que el exvicepresidente de la firma se sentía culpable por la desinformación y la mentira impulsadas por Internet. Más adelante, en ese mismo artículo, aparecía que la consultora Gartnert —yo no la conozco, pero usted sí posiblemente— dice que en el año 2022 —yo ya no estoy en Facebook, que quede claro— se consumirán más noticias falsas que verdaderas. Efectivamente, tenemos un problema, pero no es un problema otra vez de tuyos y míos; tenemos un problema en la sociedad, un problema de credibilidad, y eso se ha de atajar y se ha de trabajar con las más amplias miras posibles para no interferir en la libertad de expresión, porque hay algunos que tienen una tendencia muy clara a cortar la libertad de expresión y a que algo esté directamente controlado por el poder, sea el que sea, puede ser de cualquier país.

Dicho eso, recuerdo hace muchos años —bueno, no tantos, creo que ya teníamos euros— que a un partido político catalán que gobernaba le sobraron 6000 euros —creo que era 1 millón de pesetas, pero como no me acuerdo si eran 6000 euros o un 1 millón de pesetas doy las dos cifras— y decidió invertirlos en esto; y posiblemente fue el partido político pionero en hacer en cierta forma una fábrica de trols, y ahí no hay enemigos externos, los tenemos dentro. Hace poco un señor, Alejandro de Pedro, nos ha manifestado que tenía una granja de trols para trabajar por el buen prestigio del señor Ignacio González pero, ¿cuántos de nosotros o cuántos partidos políticos a lo mejor invierten dinero también en eso? Esa es una cosa sobre la que todos —no los tuyos o los míos sino todos— hemos de reflexionar y hemos de buscar la fórmula, que creo que debe existir o en la que, como mínimo, podemos trabajar, para potenciar aquello que es débil hoy, ¿y qué es débil hoy?, el periodismo. Hoy tenemos un periodismo muy débil y lo es porque económicamente es muy débil también. Señor compareciente, usted decía antes que se ha de

cve: DSCG-12-CM-73

buscar una fórmula, sin que sea gubernamental, evidentemente, que tenga también visión de todos nosotros, de los diferentes grupos políticos, para ayudar a aquellos que hacen una información contrastada porque, si no, nos encontraremos con que en el 2022 las noticias serán mayoritariamente falsas.

Gracias.

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

Tiene la palabra el señor Raffo.

El señor **RAFFO CAMARILLO:** Muchas gracias.

Antes de nada, quiero volver a agradecer su presencia aquí con nosotros y el esfuerzo que ha hecho personal y de desplazamiento porque nos facilita que vayamos conjugando un marco, fruto del análisis de los hechos, que nos permita después en el futuro intercambiar muchas reflexiones entre nosotros con la idea de poder plasmar algo práctico que ayude a que España esté en mejores condiciones, en colaboración y asociación con otros países de la Unión Europea y de nuestro entorno geopolítico más cercano.

Siguiendo con el asunto, esta es una periodista finlandesa. **(Muestra una fotografía).** Recibió en Suecia un premio como pudiera ser el premio Pulitzer por el gran esfuerzo y el trabajo de investigación serio y riguroso, precisamente sobre troles rusos, y le están arruinando la vida, masacrándola psicológicamente, con acoso en la red. Este es otro caso concreto y podríamos contar probablemente miles, desde ciudadanos anónimos hasta personajes políticos, periodistas, dirigentes de empresas, etcétera. Pero yo quería hacer una pregunta: ¿ha existido o existe el número 55 de la calle Savushkina? ¿Es real? ¿Existe esa sede de esa agencia que se mencionó anteriormente? **(Rumores).** Aquí es donde está localizada, según varios medios de comunicación de distintos ámbitos ideológicos y de tendencias filosóficas publicitarias, o como queramos denominarle, esta granja famosa o casa de las mentiras. Quería que, como buen analista que precisamente analiza esos flujos de información, nos confirmara que efectivamente existe un instrumento que tiene como dedicación precisamente funcionar con esas características.

Me gustaría terminar comentando una cosa. En Barcelona, recientemente, se detuvo a dos *hacker* rusos: a uno por delitos de tipo financiero, por *hackear* cuentas bancarias, etcétera, y a otro por implicación en la campaña de desinformación. Los dos están pendientes —uno creo que ya— de extradición a Estados Unidos. El abogado defensor es uno de los organizadores de un encuentro que se lleva celebrando durante dos años, 2015 y 2016, de grupos separatistas de países europeos y del ámbito mundial, entre ellos incluso de Texas y de Puerto Rico. Esta es otra información que se incorpora a una forma determinada de actuar en la que puede haber un ejército irregular —no podemos decir regular u oficial— de personas que se dedican a elaborar una estrategia en clara confrontación con lo que se denomina, entre comillas, aunque no sea hoy día exacto en un mundo globalizado, mundo occidental entendiéndolo como lo hacemos nosotros.

Nada más que esa pregunta que le he realizado sobre la calle y ese número y volverle a agradecer su presencia y que nos haya clarificado con su información muchas cosas. Muchas gracias.

El señor **PRESIDENTE:** Gracias a usted, señor Raffo.

Señor Aznar.

Señor **AZNAR FERNÁNDEZ:** Gracias, presidente.

Voy a ser muy breve, porque creo que el tiempo lo debe consumir fundamentalmente nuestro compareciente —nosotros nos conocemos todos muy bien y tenemos oportunidades varias de debatir entre nosotros—, pero quiero mencionar dos cuestiones muy concretas. Esta Comisión tiene una trascendencia más allá de las paredes del propio Parlamento, y le voy a poner un ejemplo mencionando expresamente el país al que nos hemos estado refiriendo. En la anterior sesión de la Comisión, donde compareció otra experta dándonos su opinión al respecto, la intervención de mi compañera, portavoz adjunta del Partido Popular, fue retuiteada en menos de un minuto 750 veces, atacándola. Apareció en la televisión rusa —la han convertido casi en una estrella de la televisión rusa— simplemente por venir aquí y en definitiva hablar de Rusia como país del que procedían muchos de estos ataques. Esto quiere decir que algo hay, por tanto, dejémonos ya de rasgar las vestiduras cada vez que se menciona a Rusia o a cualquier otro país, porque aquí no se ataca a nadie; estamos constatando hechos y realidades.

Para terminar, me gustaría insistirle en el tema de la colaboración ciudadana. Hemos visto y usted nos ha dado su opinión sobre lo que pueden hacer los países, las organizaciones internacionales —en este

cve: DSCG-12-CM-73

caso, la OTAN—, etcétera. Yo le menciono lo que pueden hacer los ciudadanos, más allá de la propia prensa, y creo que sería interesante en este sentido que usted nos dijera si son útiles estas organizaciones de ciudadanos. Fíjense que en algunos países se ha hablado incluso de hacer reservistas para el ejército dedicados a este tema exclusivamente.

Muchas gracias nuevamente por su comparecencia y, como ha dicho el portavoz socialista, por el esfuerzo que ha hecho desplazándose hasta aquí.

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

Doy la palabra al señor Sarts para cerrar esta comparecencia. Tiene usted la oportunidad de optar a un Oscar de Hollywood si su intervención es suficientemente escandalosa. **(Risas).**

El señor **SARTS (**Director of the NATO STRATCOM Center of Excellence): Muchas gracias por todas sus preguntas y sus reacciones.

En primer lugar, ¿cómo controlar la difusión de noticias falsas y el entorno *online* sin socavar la libertad de expresión? Creo que la forma en la que tendríamos que proceder sería, en vez de examinar el contenido —salvo que el contenido sea verdaderamente incorrecto desde el punto de vista de los hechos—, examinar más la logística. Por ejemplo, si a alguien le escucha un público de 50 000 personas, una cobertura mediática importante, ¿tenemos que pensar en aplicar las mismas leyes que si se publican noticias falsas? Todo el mundo puede cometer un error, somos personas, todos podemos cometer errores. Se puede decir: Vale, he cometido un error, lo corrijo, lo rectifico. Una de las formas en las que examinamos con quién estamos jugando es que se puede decir: Sí, hemos cometido un error; lo rectificamos. La otra forma es plantearnos si son personas reales, si la dirección es real, si existe en tiempo real. En algunos de estos casos, cuando vemos cómo se distribuye la información, no hay personas como tales o una presencia que se corresponda con cómo se está presentando en el entorno virtual.

En segundo lugar, hay que examinar siempre si hay un esfuerzo coordinado. La gente difunde rumores —eso es así—, porque somos así, las personas son así. La gente lo hace, obviamente no es lo mejor, pero tampoco hay que castigar a alguien por ello, pero si vemos que hay un actor que está realizando una acción coordinada que se puede rastrear, que está intentando tener un efecto difundiendo deliberadamente una noticia falsa o un rumor, ahí tenemos un problema. Si fueran personas reales, tal vez sería demasiado; la gente tiene derecho a expresar opiniones. Sin embargo, una vez que podamos establecer, en primer lugar, que es una realidad falsa, que no son personas, que no son organizaciones reales y, en segundo lugar, cuando veamos que hay una estrategia y no un caso de una persona individual, ahí es donde tendríamos que intervenir. Conozco a Jessikka Aro personalmente. Es una historia verdaderamente horrible de cómo esta periodista, que ha intentado demostrar lo que están haciendo los trols en Finlandia, está siendo objeto de un acoso personal de una magnitud verdaderamente dramática y creo que es un caso muy preocupante. Como decía, si un periodista está siendo acosado hasta este punto —si lo leen, verán que es una situación verdaderamente dramática y muy intimidatoria para esta joven periodista—, ahí tenemos que adoptar acciones firmes. Si además de los problemas que ya hay con el periodismo nos tenemos que enfrentar a este tipo de casos, nos vamos a encontrar con grandes dificultades.

No he estado personalmente en la calle Savushkina, pero ha habido muchos testigos de medios de comunicación occidentales que han hablado del trabajo desarrollado en este sitio y también agencias de investigación de Internet. Ha sido mencionado en una serie de publicaciones en los medios de comunicación occidentales en los que se han contado historias sobre cómo se trabaja allí. Desde mi perspectiva creo que no es necesariamente el único sitio donde se están produciendo estas cosas; nuestra premisa de trabajo es que hay más. Hace cuatro o cinco años se trataba más bien de una interacción humana —personas que escribían comentarios a cambio de dinero de forma coordinada—, pero cada vez más nos encontramos con una situación en la que es una interacción robotizada. Esto no quiere decir que se hayan eliminado todos los elementos humanos, pero creo que hay un mayor componente robotizado hoy en día. Un punto importante sobre lo que pueden hacer los ciudadanos ya se ha mencionado. Como decía, si vemos el panorama en su totalidad, apreciamos que hay una tendencia general en todas las sociedades de una disminución de la confianza en las autoridades centrales, ya sean Gobiernos, parlamentos o medios de comunicación; y esto se está produciendo en la mayoría de las sociedades que hemos examinado. Cuando analizamos en quién confían las personas, vemos que lo habitual es que confíen en el vecino de al lado o en los familiares. Este fenómeno lo están utilizando los trols, pero obviamente también quiere decir que los ciudadanos son las personas que tienen la credibilidad de cara a los demás ciudadanos. Por ello, estos movimientos de elfos en Lituania y Letonia han resultado

cve: DSCG-12-CM-73

tan efectivos, porque estas personas no reciben ningún dinero a cambio y no trabajan para el Gobierno. Creen que tienen derecho a intercambiar ideas y esto es algo que es importante. Yo sería muy prudente a la hora de decir si esto se puede hacer de forma coordinada. Creo que más bien tendría que ser un movimiento social más que algo que esté organizado y coordinado por parte de los Gobiernos. A veces, a estos grupos les interesa conocer la opinión del Gobierno y preguntan qué es lo que opina el Gobierno, pero creo que debería haber algún tipo de diferencia, división o barrera, de tal forma que no se asocie con el Gobierno. En el entorno informativo moderno el activo más importante es la credibilidad, pero también es uno de los más escasos. Ahí es donde tenemos que prestar mayor atención. Es decir, quien se enfrente a esto tiene que tener credibilidad para hacer oír su voz y para ser escuchado, porque hay muchos que no tienen esta credibilidad en la sociedad. A veces son negocios basados en un clic y los ciudadanos de a pie pueden tener un efecto inmediato. No sé si hay datos gubernamentales y los Gobiernos tal vez no puedan tener un efecto tan amplio. Se trata de que alguien independiente lo haga, y para llegar a este nivel la sociedad tiene que entender los riesgos que comporta lo que está ocurriendo para las personas y que sean conscientes de que, a lo mejor, no van a ser capaces de establecer la realidad que les rodea y que los procesos políticos y sociales también están siendo objeto de una enorme presión; hay que ser conscientes de ello. Estas serían algunas de las fuerzas más viables para solventar el problema.

Vuelvo al tema de la educación. No todo esto tiene que ser necesariamente tipo antigua escuela. Por ejemplo, nuestro centro trabaja ahora en una aplicación que convierte en un juego la capacidad, por parte de la persona que juega, de diferenciar entre la historia real y la historia no real. Es una especie de formación, una experiencia práctica, para que podamos diferenciar lo que es real de lo que no lo es. Además, como es un juego, cuanto mejor lo hagas, más incentivos vas a tener. Es una nueva forma de examinar cómo se difumina el conocimiento, y no a la antigua usanza sino de una forma más entretenida para la sociedad, que puede funcionar.

Por último, quisiera señalar que nosotros, en tanto que centro, si España entra a formar parte de él, estamos más que dispuestos a cooperar y a ayudarles en sus esfuerzos para desarrollar capacidades y enfrentarse a este problema. Estamos a su disposición. De hecho, aquí me tienen, dispuesto a ayudar a las autoridades españolas en sus esfuerzos.

Muchas gracias.

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

Damos por concluida esta primera parte de la comparecencia. Denme un minuto para acompañar a la salida al señor Sarts. En un minuto reanudamos la sesión. **(Pausa).**

— DE LA SEÑORA FISCAL DE SALA COORDINADORA EN MATERIA DE CRIMINALIDAD INFORMÁTICA (TEJADA DE LA FUENTE), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/001075 y número de expediente del Senado 713/000557).

El señor **PRESIDENTE:** Vamos a empezar la segunda parte de la sesión porque vamos con un retraso relativamente importante.

Doy la bienvenida a doña Elvira de Tejada de la Fuente, fiscal de Sala de Criminalidad Informática, a la que doy inmediatamente la palabra.

La señora **FISCAL DE LA SALA COORDINADORA EN MATERIA DE CRIMINALIDAD INFORMÁTICA** (Tejada De la Fuente): Muchas gracias, presidente.

Señorías, para mí es un placer tener la oportunidad de participar en esta sesión de trabajo y un gran honor a título personal y en mi calidad de fiscal de Sala de Criminalidad Informática, comparecer en esta ponencia. Como ustedes saben, el ministerio fiscal es una institución que tiene como funciones la defensa de la legalidad, de los derechos de los ciudadanos en el interés público tutelado por la ley. Esta función se materializa, en el ámbito de la jurisdicción penal, en el ejercicio de las acciones penales frente a todo tipo de delitos, salvo aquellos que tienen un carácter exclusivamente privado, y también en el impulso y dinamización de las investigaciones criminales y, sobre todo y muy especialmente, en la protección de las víctimas y de los perjudicados por el delito. Pues bien, el ministerio fiscal, para llevar a efecto esta función de una forma más adecuada, teniendo en cuenta la sociedad compleja en la que nos ha tocado vivir, hace ya algunos años que hizo una apuesta por la especialización. Así, tomando un poco la línea que se inició con la creación de fiscalías especiales, que sus señorías conocen perfectamente, como la Fiscalía de la

cve: DSCG-12-CM-73

Audiencia Nacional, Anticorrupción, Antidroga, se han ido creando áreas de especialización dentro de la institución a través de las cuales lo que se pretende es focalizar la atención en fenómenos criminológicos específicos. Una de estas áreas de especialización —la más joven de todas— es, precisamente, esta, el área de especialización en criminalidad informática, que tengo el honor de dirigir, que se articula en el año 2011 y empieza a andar en los primeros meses del año 2012.

Es un área de especialización que actualmente está integrada por más de ciento cincuenta fiscales, distribuidos por todo el territorio nacional; trabajamos como un gran equipo, coordinados desde la unidad central con sede en Madrid y nuestro trabajo, básicamente, es orientar, centralizar e impulsar la actuación del ministerio fiscal frente a este nuevo fenómeno criminal que es la ciberdelincuencia. Así, a partir de un esfuerzo constante de actualización de conocimientos, que he de decir que en parte es fruto de empeño propio y de recursos propios, a partir también del seguimiento de los procedimientos judiciales que se tramitan en nuestro país por hechos de esta naturaleza y, sobre todo, a partir de un trabajo muy de equipo, de reflexión, de análisis conjunto sobre la base de los conocimientos y las experiencias que vamos teniendo en el ejercicio de nuestra función, esta área del ministerio fiscal se ha convertido en una especie de punta de lanza de la actuación del ministerio fiscal frente a la ciberdelincuencia. En esta labor, nos ayudan de una forma espléndida las unidades especializadas en investigación tecnológica de los cuerpos policiales, tanto nacionales como autonómicos, que he de decir —y lo digo con orgullo— que contamos con unas unidades especializadas en investigación tecnológica con una preparación fantástica y con una capacidad profesional muy buena. También colaboramos asiduamente con organismos e instituciones nacionales e internacionales con responsabilidad en este ámbito. Por ejemplo, en el ámbito nacional, nuestra relación es frecuente con la Agencia Española de Protección de Datos, el Cnpic, el Incibe y a nivel internacional, Consejo de Europa, Eurojust, Interpol, Europol, etcétera. También la fiscalía está haciendo —quiero destacarlo— un esfuerzo importante por acercarnos a la sociedad que pudiéramos llamar civil, entre comillas, es decir, a las entidades del sector privado, a los ciudadanos, desde el entendimiento de que su papel puede ser también de gran importancia en la lucha contra la ciberdelincuencia.

Ahora, seis años después de haberse creado está área de especialización, permítanme que me enorgullezca de esa decisión ya que creo que optar por esta área de especialización fue una apuesta valiente de la fiscalía, porque es evidente —lo estamos viendo todos— que es necesario construir entre todos estrategias que nos permitan, por una parte, garantizar o al menos hacer posible un uso seguro del ciberespacio y, al mismo tiempo, tener una línea de actuación eficaz frente a la ciberdelincuencia, como dos factores que deben ir íntimamente vinculados. Ustedes saben bien, porque por eso forman parte de esta ponencia y en ello están trabajando, la incidencia que toda la evolución tecnológica está teniendo en nuestra vida y en el funcionamiento de la sociedad, en general con efectos positivos, sin duda, pero también se están produciendo efectos perversos. Uno de esos efectos es, justamente, la incidencia que todo este desarrollo tecnológico está teniendo en la delincuencia. Al hilo de ese desarrollo tecnológico están surgiendo conductas nuevas, impensables hace veinte o treinta años y que por eso no estaban previstas como delitos en los ordenamientos jurídicos de los Estados y que, sin embargo, se están produciendo y que son capaces de lesionar y muy gravemente bienes jurídicos necesitados de protección. En otros casos lo que estamos viendo es aparecer nuevas formas de planificar y desarrollar delitos tradicionales, que ya estaban en los ordenamientos jurídicos pero que ahora se cometen de otra forma distinta, merced al uso de estas herramientas tecnológicas. En uno y en otro caso esto demanda una evolución de los ordenamientos jurídicos para ofrecer respuestas legales ante esas nuevas situaciones.

Otro gran ámbito que supone un desafío importante es la investigación de estas conductas, la investigación tecnológica. A nadie se le escapa que investigar un delito que se comete en el ciberespacio solo puede llevarse a efecto a través del propio ciberespacio, es decir, utilizando los sistemas informáticos, utilizando las propias tecnologías como elemento de investigación criminal. Tenemos que hacerlo y, además, de una forma eficaz, pero tenemos que hacerlo sin que ello suponga afectar o limitar los derechos y las libertades fundamentales que podrían verse afectados como consecuencia de ello: derecho a la intimidad, privacidad, protección de datos, secreto de comunicaciones, etcétera. En definitiva, lo que les quiero trasladar es que nos encontramos ante un fenómeno muy vivo, que evoluciona muy deprisa, muy abierto y muy transversal. Cuando hablamos de ciberdelincuencia en realidad no estamos hablando de una categoría cerrada y predeterminada de delitos, como cuando hablamos, por ejemplo, de delitos contra la seguridad del tráfico, sino que estamos hablando de una forma de cometer delitos de muy distinta naturaleza. Ciertamente, lo que es el corazón de la ciberdelincuencia son los delitos que se cometen desde las tecnologías contra los elementos y los sistemas informáticos, pero todos somos conscientes de

cve: DSCG-12-CM-73

que se están aprovechando las potencialidades que ofrecen las herramientas tecnológicas para cometer actividades ilícitas muy diversas, que afectan a bienes jurídicos, por ejemplo, personales —la intimidad, el honor, la libertad e indemnidad sexual de los menores—; en otros casos a bienes de carácter patrimonial, y ahí tenemos las estafas o los sabotajes informáticos y, en ocasiones, a intereses de carácter general, supraindividuales, y el mejor ejemplo que se me ocurre es, sin duda, la utilización de Internet con finalidades terroristas.

La fiscalía, a partir del trabajo que ha venido realizando a lo largo de estos seis años como área de especialización, ha recopilado información sobre toda esta fenomenología criminal. No es una información completa, lo digo claramente, pero sí una información veraz y suficientemente contrastada sobre cómo está evolucionando este fenómeno criminal y sus distintas manifestaciones. Me van a permitir que, muy brevemente, les haga un dibujo a grandes trazos de esta fenomenología criminal. En primer término, las conductas que con más frecuencia se denuncian ante los tribunales de entre las que se cometen a través de las TIC son, sin duda, las estafas o defraudaciones. De hecho, les diré que el año pasado, según la memoria de la Fiscalía General del Estado, el 61 % de los procedimientos judiciales incoados por ciberdelitos fueron por tipos penales de esta naturaleza. Ahora, hablo de estafas en un sentido muy amplio que incluye tanto la estafa tradicional, es decir, la oferta fraudulenta de bienes y servicios que ahora se hace a través de la red, lo que determina que el número de perjudicados se haya incrementado de una forma exponencial, como otras formas mucho más sofisticadas de defraudación, como, por ejemplo, las transferencias económicas inconsentidas utilizando claves bancarias sustraídas a sus legítimos usuarios, bien sea por procedimientos delictivos multietapa como el *phishing*, o bien sea a través de ataques de espionaje informático; o la utilización fraudulenta de tarjetas de crédito o débito o de sus datos, el conocido como *carding*; o los distintos tipos de defraudación en relación con la contratación irregular de servicios de telecomunicaciones, básicamente de telefonía.

A la fiscalía uno de los aspectos que más le preocupa es todo el tipo de actividades delictivas que se cometen a través de la red y que inciden en la libertad e indemnidad sexual de los menores. Me estoy refiriendo concretamente a delitos relacionados con la distribución y fabricación de pornografía infantil y también al *child grooming*, el acoso a menores a través de Internet con fines de carácter sexual. Desgraciadamente, son conductas que se han visto incrementadas y muy favorecidas por dos circunstancias que son evidentes: por una parte, la potencialidad que ofrecen estas tecnologías para facilitar la comunicación entre personas y, por otra parte, el uso generalizado de estas herramientas por nuestros chavales, que se han convertido en víctimas muy, muy vulnerables frente a este tipo de comportamientos. Son conductas cuya investigación presenta mucha complejidad y, además, esa complejidad se ve incrementada por el hecho de que, como se van sofisticando los medios de comunicación, esos nuevos medios de comunicación se están utilizando para la distribución por ejemplo de material pornográfico. Las últimas investigaciones que estamos abordando son distribución de pornografía infantil en la *deep web* y también a través de los sistemas de mensajería instantánea de Whatsapp y de Telegram, donde la investigación puede resultar bastante más compleja.

También quería referirme como otra forma de actividad delictiva que creo que tiene mucha importancia, a los delitos relacionados con los ataques a los sistemas de información, tanto ataques de espionaje informático como ataques de sabotaje informático. Fíjense que en el año pasado se incoaron 682 procedimientos judiciales por hechos ilícitos de esta naturaleza. La cifra —yo creo que es muy pequeñita— deja constancia de algo importante: que no se está poniendo en conocimiento de los órganos de la jurisdicción penal este tipo de conductas. Es decir, los ataques informáticos no se están denunciando, por razones reputacionales o de otra índole, no voy a entrar en ello, pero lo cierto es que no están llegando a conocimiento de los órganos de la jurisdicción penal. Esto, desde mi punto de vista, es preocupante y por eso llamo la atención de sus señorías sobre ese extremo en el entendimiento de que una actuación eficaz frente a los ataques informáticos exige combinar la acción preventiva, que es muy importante, con el ejercicio de la acción represora del Estado cuando esos hechos sean delictivos, que tengamos capacidad de reaccionar para evitar la impunidad de esas conductas. Confiamos en que la implementación en el ordenamiento jurídico interno de la Directiva NIS y en consecuencia de la obligación de notificar incidentes de seguridad —que se va a establecer para determinados operadores esenciales—, facilite que esa información llegue hasta los órganos de la jurisdicción penal para que podamos ejercer acciones penales frente a esos comportamientos. De hecho, me atrevería a sugerir a sus señorías que, cuando esa ley de implementación de la Directiva NIS se vea en estas Cámaras, se cuide especialmente que se recuerde la obligación que tienen esas autoridades públicas que reciban la notificación de

cve: DSCG-12-CM-73

incidentes, de dar traslado de esos incidentes a los órganos de la jurisdicción penal cuando los hechos revistan los caracteres de delito.

La fiscalía está dispuesta a poner nuestro granito de arena en ese proceso y de hecho acabamos de publicar una circular, 3/2017, en la que analizamos en profundidad estos tipos penales, justamente para facilitar que aquellos que van a recibir esta notificación de incidentes tengan criterios para poder deslindar cuáles de esos incidentes de seguridad pueden ser delictivos y puedan en consecuencia llevar a efecto ese traslado de información a los órganos de la jurisdicción penal.

No quiero cansar a sus señorías, pero tengo que referirme cuando menos muy brevemente a otras figuras delictivas que se están dando con mucha frecuencia en la red y sobre las que me gustaría llamarles la atención: delitos contra la libertad y seguridad de las personas, amenazas, coacciones, acoso —todos los días, y de esas conductas muchas veces las víctimas son precisamente los más vulnerables, menores y víctimas de violencia de género, entre otros— delitos contra el honor, difusión a través de las redes de conductas de carácter injurioso o calumnioso, que exceden en mucho en sus contenidos de los límites que tienen las libertades garantizadas en el artículo 20 de la Constitución española; delitos de odio, difusión en la red de mensajes o consignas que incitan al odio, a la discriminación o a la violencia respecto de los que son diferentes por la raza, por el color de su piel, por su situación económica, por su orientación sexual, por sus creencias religiosas, por cualquiera de los motivos. Estos delitos presentan problemas importantes en su investigación y hay que actuar con rotundidad frente a ellos porque socavan los valores de las sociedades democráticas. A las dificultades que presenta la investigación de estas conductas se une otra, y es que muchas veces estos contenidos se están difundiendo a través de redes sociales o de plataformas cuyos responsables radican en otros Estados y respecto de los cuales la capacidad de imponer decisiones de las autoridades nacionales presenta problemas. Este es un tema que está preocupando mucho a nivel de la Unión Europea. De hecho, se está trabajando en ello tanto en el ámbito de la Unión Europea como del Consejo de Europa, intentando crear reglas de conducta que nos permitan por lo menos retirar aquellos contenidos que sean especialmente perversos, especialmente delictivos.

Me gustaría hacer una breve referencia —no voy a extenderme sobre ello porque no es el área de mi especialidad, es competencia de la Fiscalía de la Audiencia Nacional, pero no puedo dejar de mencionarlo— a la utilización de Internet con finalidades terroristas. Ustedes lo saben bien, la utilización de todas estas capacidades para encontrar terroristas, para adiestrarlos, para entrenarlos, para difundir mensajes que incitan a la comisión de actos de terrorismo es un gran problema. Lo tenemos ahí y tenemos que actuar frente a él. Este es un poco el panorama general.

Respuestas. Desde nuestra experiencia yo daría dos grandes líneas de actuación tal como nosotros lo vemos: en primer lugar, una respuesta en el ámbito puramente legislativo, es decir, el ordenamiento jurídico tiene que evolucionar constantemente para ir articulando los mecanismos legales que nos permitan actuar en vía penal frente a estos comportamientos; y en segundo lugar, en el ámbito operativo, es decir, hay que reforzar la capacidad operativa de las unidades, de los órganos de investigación, de los órganos de enjuiciamiento, de los operadores jurídicos que se ocupan de luchar contra la ciberdelincuencia. Yo llamaría la atención sobre los aspectos formativos. Hay que invertir seriamente en formación a distintos niveles y también hay que dotar de medios personales y materiales a las unidades de investigación, a los laboratorios de policía científica y de criminalística, a las fiscalías, a los operadores jurídicos en general.

Centrándome ya en los aspectos legislativos, que son los más propios de este foro, permítanme una reflexión personal al respecto. Entendemos que esa evolución legislativa a la que me refería debería hacerse muy coordinada con la evolución que a su vez están llevando otros países, en particular los de nuestro entorno más próximo, siguiendo las directrices y pautas internacionales. No en vano estamos ante un fenómeno que trasciende las fronteras de los Estados y ante el que hay que reaccionar de una forma coordinada. Si no, estamos perdidos. Por eso es importante que las legislaciones de los distintos Estados se aproximen lo más posible para que tengamos ese —¿cómo diría yo?— lenguaje común que nos permita trabajar juntos de una forma más fácil. En eso se está trabajando mucho en todos los ámbitos geográficos. En la Unión Europea hay muchas iniciativas —no podría entrar a valorar ni a analizar todas ellas—, igual que en el Consejo de Europa. Aquí quería pararme un minuto, porque quería hacer referencia a la Convención de Budapest del Consejo de Europa, que es un documento yo creo que de gran importancia en la lucha contra la ciberdelincuencia. Es del año 2001, España lo ratificó en el año 2010 y actualmente lo han ratificado cincuenta y seis países de distintas áreas geográficas del mundo. En esta convención España se encuentra muy implicada, tanto en el desarrollo y avance de los propios planteamientos de la convención como en la incorporación al ordenamiento jurídico de sus directrices.

cve: DSCG-12-CM-73

Fíjense en que la Convención de Budapest tiene dos grandes objetivos: uno, la armonización normativa —a la que ya me he referido y además en los mismos términos—, y dos, que también es muy importante, el reforzamiento de la cooperación internacional, donde tenemos otro gran desafío. Justamente ahora estamos trabajando en la convención en un segundo Protocolo Adicional a la Convención de Budapest, con dos líneas de acción especialmente importantes, entre otras: primera, mejorar las herramientas de cooperación directa entre autoridades judiciales y policiales de los distintos Estados en la lucha contra la ciberdelincuencia, y, segunda, articular mecanismos de cooperación con el sector privado —a lo que se le está dando una gran importancia—, en particular, operadores de comunicaciones y proveedores de servicios de Internet. Tengo que decir con orgullo que la legislación española en esta materia está muy bien, está en una línea muy adecuada; es una legislación muy adaptada a las necesidades reales en la lucha contra la ciberdelincuencia. Gracias al esfuerzo que se ha hecho en estas Cámaras y, sin lugar a dudas, al impulso de los Gobiernos, se han llevado a efecto dos importantes reformas del Código Penal: una en el año 2010 y otra —dos, en realidad— en el año 2015, que han hecho que nuestras figuras delictivas estén plenamente adaptadas a las directrices internacionales.

En cuanto a la investigación tecnológica, he de decir lo mismo. Pese a que nuestra Ley de Enjuiciamiento Criminal es muy antigua —es de finales del siglo XIX—, lo cierto es que hubo una reforma muy importante en el año 2015 que se ocupó de toda la investigación tecnológica y que reguló al detalle el uso de las herramientas tecnológicas como medio de investigación criminal. De hecho, tenemos reguladas instituciones, como el agente encubierto *online* o el registro remoto de sistemas, que están sirviendo de fuente de inspiración a los legisladores de otros países porque son herramientas de investigación muy vanguardistas. Pero nunca se puede decir que el trabajo está terminado, y menos en esta materia, en la que la evolución tecnológica hace que evolucione la situación fáctica y, como he dicho antes, el ordenamiento jurídico nunca puede estar parado. Por eso, me van a permitir que en tres minutos les resuma tres iniciativas o sugerencias que me gustaría hacerles de modificaciones legislativas que parten de nuestra experiencia como fiscales, es decir, de necesidades que estamos detectando y que sería bueno abordar.

La primera de ellas —en relación con ello desde la fiscalía se ha hecho algún pronunciamiento, incluso ante estas Cámaras— es la tipificación penal de la figura de la suplantación de identidad en la Red. Me estoy refiriendo a los supuestos en los que una persona se hace pasar por otra realmente existente en todo su haz de relaciones —sociales, personales— en la Red. Esto suele dar la capacidad, primero, de inmiscuirse en su ámbito de relaciones y, además, de asignar a la persona suplantada pensamientos, reflexiones u opiniones que no se corresponden con la realidad y que pueden llegar a hacerle desmerecer en su consideración pública o en el respeto debido por los demás. Son conductas que hoy en día tienen una difícil respuesta con el Código Penal actualmente vigente. Ciertamente, la suplantación de identidad en algunos casos sí puede perseguirse: cuando se utiliza como medio de estafa, sí, pero se persigue como defraudación; cuando se utiliza como medio para cometer un ataque informático, también, pero se persigue como ataque informático. Tal vez sería conveniente tipificar específicamente la suplantación de identidad en aquellos supuestos en que la lesión que se produce es la que les he dicho: sencillamente, la relativa al bien personal, la privacidad, la intimidad, el derecho al respeto, a la dignidad propia, a la consideración individual.

Otra sugerencia de modificación está relacionada con los delitos de injurias y calumnias, a los que me he referido anteriormente. Como les he dicho, son delitos que se están dando con muchísima frecuencia en la Red —ustedes lo saben muy bien— y que, como también saben, en la mayor parte de los supuestos son de carácter privado. Es decir, solamente se pueden perseguir cuando se querella el ofendido, no tiene intervención en ministerio fiscal. Ya nos hemos encontrado en varias ocasiones —y seguramente sus señorías lo recordarán— algunos supuestos en los que el ofendido había fallecido; es más, en ocasiones, la campaña de injurias o calumnias se produce a raíz del fallecimiento del ofendido. En estos casos la acción penal está vetada porque el ofendido no puede ejercitarla y los herederos o familiares del ofendido están abocados a irse a la vía civil si quieren enmendar esas situaciones. Al respecto, me parece oportuno recordarles a sus señorías que en el Código Penal anterior al actualmente vigente —me refiero al Código Penal del año 1973—, en el artículo 466 se contemplaba la posibilidad de que en los casos de fallecimiento, en determinadas circunstancias y por determinados plazos, los familiares o los herederos del fallecido pudieran ejercitar la acción penal y se me ocurre que tal vez sería conveniente rescatar aquella posibilidad para dejar abierta esta vía en el Código Penal actualmente vigente.

cve: DSCG-12-CM-73

Finalmente, haré una tercera sugerencia relacionada con la reiteración que venimos observando en determinados comportamientos en la Red. Fíjense en que hay conductas —me refiero, por ejemplo, al acoso a menores a través de Internet, me refiero a la distribución de pornografía infantil e incluso me refiero a algunos supuestos de delitos contra la propiedad intelectual— cuyos autores reiteran el comportamiento en el tiempo una y otra vez. Para estos supuestos, en la fiscalía nos habíamos planteado que sería conveniente, además de la pena de multa o de prisión prevista en cada supuesto, poderles sancionar con una pena de prohibición de utilización de Internet, de acceso a las redes o de administrar páginas web. Es una sanción que tendría dos efectos: el represivo propiamente dicho, pero, además, un efecto de prevención especial y general muy importante. Nosotros estamos intentando hacerlo valer amparándonos en una interpretación abierta de algunos preceptos del Código Penal, pero con poco éxito, se lo tengo que confesar. Tal vez sería inconveniente incorporarlo como pena específica que podría salir al paso de algunos de estos supuestos.

Quiero hacer una última precisión de carácter general. Se encuentra sin ratificar el Segundo Protocolo Adicional al Convenio europeo sobre asistencia mutua en materia penal del Consejo de Europa. Me consta que desde la Comisión de Asuntos Exteriores se ha instado la culminación de ese trámite y nosotros querríamos trasladar la oportunidad de que se culmine ese proceso. Efectivamente, no es una herramienta específicamente destinada a la lucha contra la ciberdelincuencia pero sí a la cooperación internacional contra la delincuencia en general. Ahí hay algunas herramientas, como la posibilidad de utilizar equipos conjuntos de investigación, que nos hemos visto privados de utilizar precisamente porque ese protocolo no estaba ratificado.

Termino. Quiero agradecer la oportunidad de estar entre ustedes y poder trasladarles nuestras inquietudes, nuestras opiniones y nuestro punto de vista. También quiero decirles que, por supuesto, estoy a su disposición para todo aquello que quieran comentar o para las sugerencias que nos quieran hacer llegar.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señora Tejada de la Fuente.

Estoy seguro de que muchas de las sugerencias, sobre todo en lo que se refiere a los cambios legislativos, podrían formar parte de este final de la ponencia como sugerencias de esta Comisión, porque han sido, en mi opinión, inteligentes.

Comenzamos en turno de portavoces dando la palabra al señor Legarda.

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

Muchas gracias, señora fiscal, por la exposición que nos ha realizado. Es difícil intervenir tras una exposición notablemente técnica. Voy a plantearle alguna cuestión y a pedirle su opinión respecto de un problema que veo que es consustancial al derecho penal y a la ciberseguridad y que, además, es de difícil solución. El derecho penal que conocemos, que hemos aprendido y que ejercitamos es un derecho penal sobre todo de base territorial. Y nos encontramos con una realidad que es de base extraterritorial, no solo porque digamos que es internacional; es que el elemento territorial está difuminado o es un territorio que nosotros todavía culturalmente no lo visualizamos como territorio porque no tiene realidad física. Quizás vayamos construyendo un concepto del territorio distinto, porque el territorio en el que vive el Código Penal es un territorio físico. Podemos cooperar internacionalmente, pero cooperamos siempre sobre realidades territoriales, físicas. No voy a minimizar la utilización de las tecnologías para la comisión de delitos individuales, como muchos de los que se denuncian. Me estoy refiriendo a la ciberseguridad relacionándola con aquella criminalidad que usa la Red porque es una criminalidad organizada y que tiene una base territorial muy difusa. Y también la que afecta a medios tecnológicos, donde el efecto se produce en un territorio pero el ataque no, la trazabilidad y la determinación de la autoridad es prácticamente imposible. Se puede determinar más o menos del área de donde ha venido, pero no la autoría. La duda que tengo es si realmente tenemos herramientas para combatir esta nueva tipología, que es un instrumento pero que también es una tipología delictiva; si estamos preparados intelectual, cultural o civilizatoriamente.

La segunda cuestión es si cuando vayamos construyendo ese nuevo derecho penal, basado en una realidad inmaterial pero una realidad al fin y al cabo, no caminaremos sobre una línea en la que ya está caminando el derecho penal. El derecho penal clásico era un derecho de respuesta ante conductas. Ahora está migrando, está yendo hacia un derecho de riesgo, que es preventivo; un poco el *minority report*. No sé si esta realidad sobre la que vamos a tener que trabajar nos va a llevar —es mi pregunta, mi reflexión

cve: DSCG-12-CM-73

y quiero saber qué opina usted— hacia un derecho penal desconocido, hacia un derecho penal de riesgo más que a un derecho penal sobre la conducta. Esas eran mis preguntas.

Muchas gracias.

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

Señor Salvador.

El señor **SALVADOR GARCÍA:** Gracias, presidente.

Muchas gracias, por la comparecencia, señora Elvira. Sobre todo, me ha gustado mucho el marco que ha expuesto porque es absolutamente realista y demuestra la especialización de lo que usted está gestionando y su importancia. Yo conozco muy bien el trabajo de Paco Hernández, que es el fiscal de Granada, que está haciendo una labor impresionante. Es verdad que lo primero que tiene que conseguir esa especialización es que el resto de colegas entiendan que los tiempos y modos de funcionamiento de un fiscal especializado en este tipo de delitos es distinto, por la propia tipología de los delitos, a los de otros delitos que se cometen en el mundo real, fuera de la virtualidad. En ese sentido, quiero mostrar el apoyo de nuestro grupo a su trabajo y a la necesidad de una mayor especialización del número de personas que puedan contribuir para agilizar este tipo de procedimientos.

Usted misma se ha contestado preguntas propias que podíamos haberle formulado, porque ha ido dando las soluciones y, sobre todo, ha terminado con esa parte, en la que yo coincido con el presidente, que tendríamos que incorporar. En eso me voy a centrar un poco más de entre todas las tipologías que ha mencionado de delitos. Es verdad que si se produce, por ejemplo, una estafa masiva, como es masiva, se tiende a actuar para solucionarla porque a lo mejor afecta a 30 000 o 50 000 personas. En relación con la seguridad del sistema financiero —que son los primeros que están invirtiendo lo máximo posible para tratar de garantizar la seguridad—, ha expuesto algo que es fundamental. Si se pueden robar contraseñas y si a partir de ahí se pueden hacer transacciones económicas, entonces debemos conseguir la seguridad absoluta para poder operar. Cuando voy a un banco y me identifico en ventanilla o saco dinero con mi tarjeta y pongo un código no puedo sacar más que una cantidad máxima de dinero en una transacción para garantizar que si alguien me roba la tarjeta no pueda sacar más de esa cantidad, pero cuando se produce en el ámbito de la Red, la información está absolutamente encriptada y protegida, pero si luego eso se lo roban del servidor al banco o al operador y pueden utilizar los datos de las tarjetas bancarias, tenemos un problema. Tengo la sensación de que se está intentado actuar lo antes posible en ese tipo de delitos y de actuaciones y que hay un grado de sensibilización bastante importante. Las aportaciones que hace sobre los cambios legislativos que son necesarios tienen que ver precisamente con el tema de la suplantación de identidades en la red, el tema de las injurias y calumnias, y la reiteración de conductas.

Le voy a contar, muy por encima, algo muy cercano. Puede ocurrir en un momento determinado que una persona, de repente, puede suplantar la figura de otra persona distinta haciéndose pasar por ella; puede haber pruebas en la Red de que esa suplantación es absolutamente real; una persona puede, de repente, crear un mundo imaginario de otros muchos personajes que no existen, pero que, supuestamente, tienen interrelación y que interactúan con la gente, sobre todo con la persona o personas que pretenden acosar; y todo ese universo está actuando. Hemos hablado de personas vulnerables, de niños, de menores y también ha dicho antes que muchas empresas no denuncian por el tema de la reputación, porque si se sabe que esa empresa es vulnerable o ha podido tener un problema, eso puede tener un efecto derivado muy importante en la pérdida de negocio por la pérdida de confianza. Eso pasa también con muchas personas que tienen representación pública y se ha de intentar salvaguardar ese honor, esa intimidad y esa reputación. Recientemente, en este Congreso, se manda a una Comisión un correo sin firmar, sin ningún tipo de autenticidad, donde se pide que a un partido se le excluya del pacto contra la violencia de género porque se ha denunciado a un diputado por una asociación de Madrid para la defensa de las mujeres víctimas de la violencia de género. Eso se manda a todos los miembros de una Comisión, se manda a distintos partidos políticos y a mucha gente, y el diputado se entera porque un amigo le dice lo que le han enviado. Cuando lo llevas a la policía para poner una denuncia, se certifica, primero, que a esa persona no la ha denunciado nunca nadie por violencia de género, que esa asociación no existe y que es un bulo que circula que puede estar, incluso, en esta misma casa. Eso da lugar a que, en un momento determinado, la gente se pregunte si habrá hecho esto, si le habrán denunciado o no. Por ello, creo que las medidas que está usted aportando en este momento son realmente urgentes, porque no hay capacidad de actuar.

cve: DSCG-12-CM-73

Por ejemplo, en cuanto a la reiteración de conductas, en el caso al que me estoy refiriendo hay una persona que fue denunciada, fue detenida por la policía, se verificaron los hechos, se dictó una orden de alejamiento de comunicaciones, a propuesta del fiscal, por el propio juez. Todo eso existe y, sin embargo, esa persona sigue manejando, sigue gestionando las redes y sigue haciendo las mismas cosas; es una persona que no está equilibrada mentalmente y, por tanto, es susceptible de reiterar los acontecimientos, a pesar de que se tenga constatación de que esas cosas suceden. ¿Cuál es la experiencia que he visto también en la relación entre policía y justicia sobre todo esto? Pues que cuando se trata de temas que afectan, por ejemplo, a políticos, al estar acostumbrados a que haya muchos bulos, muchas historias y muchos ataques para distorsionar la imagen de las personas públicas, los jueces o la gente que aborda esos casos piensan que es el lío de la política, y rápidamente se cierran y no se avanza en la investigación.

Por tanto, quiero decirle que mi grupo comparte totalmente la definición que ha hecho; repito, creo que necesitan todavía más medios; que estos cambios legislativos que usted está proponiendo son absolutamente necesarios y trabajaremos con el presidente de nuestro grupo para corregirlo, porque si no se corrige esto, cualquier persona es absolutamente vulnerable. Si lo puede ser una persona relacionada con estas Cortes Generales, imaginemos una persona del mundo civil a la que de repente le caiga algo encima que no sepa de dónde viene. El nivel de acoso y el impacto sobre la reputación y la imagen puede ser tremendo.

Le animo a que siga su camino y nosotros, desde esta Cámara, vamos a estar abiertos tanto a estas tres propuestas concretas que usted ha hecho sobre cambios legislativos como a cualquier otra que entienda que puede mejorar realmente la seguridad en la Red, que es lo que finalmente perseguimos, para que sea confiable y que proporcione avances para la sociedad, que es lo que creo que necesitamos en este momento.

Muchas gracias.

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

Tiene la palabra el senador Comorera.

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

Muchas gracias, señora Tejada de la Fuente, por la magnífica comparecencia y por su exposición, que, como señalaba el señor Salvador, ya ha respondido a muchas de las preguntas que al menos yo me había preparado para formularle.

Una de las cosas que me preocupan —aunque ya ha matizado usted la necesidad de incrementar los medios— es si realmente tenemos una fiscalía adaptada para luchar contra estas nuevas formas de criminalidad que poco a poco van rellenando lo que antes —hace unos cuantos años— era una parte muy pequeña, y vemos cómo una gran parte de los delitos tienen este componente de cibercriminalidad. Yo he conversado con algunos fiscales sobre este tema y la mayoría reflejaba la necesidad de medios materiales —lo cual es evidente—, pero también de formación. Me contaban que, respecto a los medios informáticos necesarios para su trabajo, carecen de la tecnología adecuada; me explican que ellos van en Seat 600, mientras que los ciberdelincuentes muchas veces van en Ferrari, y eso es una realidad. Por otra parte, también criticaban que se les daba alguna formación a los delegados, pero el resto de fiscales prácticamente no tenían ningún tipo de formación con relación a la cibercriminalidad. Y ya no solo los fiscales, sino que los propios jueces también criticaban este aspecto y me ponían el ejemplo de algunos jueces que no sabían distinguir entre Facebook y Twitter o lo que era un DM privado —es decir, cosas muy básicas— y que se veían con problemas en los juicios orales, por ejemplo, para hacerse entender. También señalaban que a la hora de proponer las pruebas tenían mucha dificultad para que los jueces entendieran qué es lo que la fiscalía les solicita, porque no entienden. Me gustaría que me diera su opinión sobre si, no solo al departamento que usted representa sino a la fiscalía y a la judicatura en general, les tendríamos que dar muchas nociones en esta materia, toda vez que esto irá en aumento en los años venideros.

Por otra parte, me gustaría saber si tienen algún sistema de control en cuanto a los delitos o las infracciones leves, sobre todo con relación a las estafas, que permita establecer relaciones entre unos y otros. Nos preocupa mucho que estas pequeñas estafas, que no llegan a las cantidades requeridas, muchas veces queden muy difuminadas. Esta es una realidad que también nos preocupa. Asimismo, me gustaría saber qué problemas generan para la fiscalía las operaciones defraudatorias que ha comentado antes de carácter multietapa —sobre todo el *phishing*—, tanto por la frecuencia como por los problemas que ocasiona.

cve: DSCG-12-CM-73

Para acabar, en cuanto al tema de los delitos de odio a través de las redes sociales, me gustaría saber qué criterios sigue la fiscalía respecto a qué se persigue y qué no se persigue. Los que estamos acostumbrados a navegar por las redes nos damos cuenta de que no es difícil encontrarse con algo que podría ser considerado como un delito de odio. Es imposible ponerse a perseguir absolutamente todo: seguramente ni la fiscalía ni los jueces tengan tanta capacidad. Por tanto, me gustaría saber qué criterios sigue la fiscalía para determinar lo que persigue y lo que no.

Muchas gracias.

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

Señor Luena.

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

Gracias, señora Tejada de la Fuente —paisana—, bienvenida; y le doy las gracias, además, por la cantidad de información que nos ha trasladado. Como decían ahora algunos portavoces, es verdad que gran parte de las preguntas que teníamos preparadas ya han sido respondidas en su primera intervención, lo cual se agradece, y descuide, porque incorporaremos las distintas sugerencias que nos ha hecho. Nos vamos a interesar particularmente por la ratificación del protocolo al que usted se refería; supongo que lo hará la Comisión y, si no, el Grupo Parlamentario Socialista lo hará. Ya que ha entrado usted en materia de legalidad, nos gustaría saber de qué forma ha colaborado en la trasposición de la Directiva comunitaria de ciberseguridad, en qué contenidos concretos y si le consta que el Gobierno va a tener en cuenta sus criterios. Por la actitud que le hemos visto en esta comparecencia, nos ha quedado claro que usted le ha hecho llegar al Gobierno bastantes sugerencias. Como va a venir aquí el texto —ya que nos ha puesto deberes, permítame que le ponga yo uno—, podría irnos adelantando qué prioridades le ha dado al Gobierno para que también nosotros, sobre todo los grupos de la oposición, podamos tenerlo en cuenta.

Dicho esto, permítame una ráfaga de preguntas. Le decía que muchas de ellas ya las ha respondido y le pediré más concreción, pero son rápidas y breves. En cuanto a las prioridades de la fiscalía, ¿hay algún mecanismo para abordarlas o es usted quien fija las prioridades de actuación de la fiscalía? Ha sido usted bastante clara con los medios y los recursos materiales y humanos. Nos ha quedado a todos claro que son necesarios más refuerzos, tanto operativos como de formación. En ese sentido, le pregunto si existe algún programa concreto de formación y sensibilización continuado para jueces y fiscales en esta materia. Nos ha hablado de la tipología de los delitos, pero no de su evolución. Me gustaría que nos pudiera comentar *grosso modo* la evolución, porque nos ha hecho una clasificación bastante sucinta. ¿Tienen ustedes alguna memoria anual o han pensado en ello? Sería bueno que de esto también hablásemos. No nos ha hablado del Centro Criptológico Nacional, aunque entiendo que existe una coordinación habitual entre la fiscalía y el centro. Sobre ciberespionaje, aunque lo ha mencionado de pasada, le pregunto si hay alguna coordinación sistémica concreta establecida entre el Gobierno, la fiscalía y las empresas estratégicas. ¿Existe como *modus operandi* habitual? No sé si nos puede decir cuántas redes de delincuencia en el ciberespacio están detectadas en España, más o menos.

Entramos ya en la jerga que se va haciendo muy específica de esta materia. En relación con los «hacktivistas», le pregunto cuál es la situación actual, los casos en la justicia y las personas condenadas. Sería bueno para la ponencia y para nuestro trabajo que tuviéramos esta información.

Voy terminando, señor presidente. Ciberyihadismo, ¿qué actuaciones se están realizando —hasta donde nos pueda decir, porque comprendemos la sensibilidad— y qué medios están utilizando ante esta amenaza creciente, como usted ha reconocido en la parte final de su comparecencia? Termino con una parte sobre las herramientas —cada vez hay más— que son capaces de monitorizar el tráfico de red. Usted lo ha dicho de pasada, pero ¿existe una relación y una colaboración con las grandes compañías tecnológicas para combatir estos delitos? Por cierto, ¿hay alguna denuncia sobre posibles incumplimientos de la legalidad de estas compañías en cuanto al uso fraudulento de los datos? ¿Existen denuncias concretas? Acabo con una sugerencia y una reflexión que se va haciendo ya casi tradicional en esta Comisión. La sugerencia es que quizás pertenece más a esta casa y le pido que nos dé su opinión sobre si sería bueno que con un carácter semestral o anual usted viniera a esta Comisión y nos hiciera un balance. Si todos estamos de acuerdo en la importancia y la prioridad que tiene esta materia, quizá es bueno que la pongamos también entre las prioridades de las Cortes Generales.

Termino. No sé si usted es experta —no tiene por qué serlo— o conoce la ornitología, pero últimamente en nuestra Comisión hablamos mucho de aves, concretamente de patos. Me gustaría que nos diera una opinión, aunque no la quiero meter en ningún lío ni quiero que usted comience ningún conflicto diplomático.

cve: DSCG-12-CM-73

Se habla mucho, por resumirlo, de la injerencia rusa o ruso-venezolana en la situación política catalana, por definirlo así, y usted ha hablado en una parte de su intervención de los nuevos fenómenos criminales. En la última sesión compareció la señora Milosevich-Juaristi, del Real Instituto Elcano, y nos vino a decir —mi compañero el senador Raffo me hablaba de los 4800 bots que jalearon el *procés*— que la cosa apuntaba maneras. Después, nuestro portavoz, el señor Hernando, vino a explicar que cuando todas las cualidades de un animal parece que indican que es un pato, a ver si al final acaba siendo un pato. Lo que yo querría saber es su opinión, porque hemos podido ver que tiene bastante dominio de la materia, sobre esta supuesta injerencia rusa en la situación política de Cataluña y si en algún momento —como le decía, no la quiero meter en ningún conflicto diplomático— podría haber habido algunas actuaciones que puedan ser constitutivas de delito.

El señor **PRESIDENTE:** Por el Grupo Parlamentario Popular, señora Vázquez.

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

Doy la bienvenida a esta Comisión a la señora fiscal, cuya intervención ha sido brillante, como no esperábamos menos de usted, sin lugar a dudas. Yo no le voy a hablar de los rusos, porque la última vez que hablé de los rusos salí varios días seguidos en la televisión rusa, así que voy a hablar de España, de este país que tiene más de veintiocho millones de usuarios de Internet, es decir, casi el 80 % de la población está conectada dos o tres veces a la semana a Internet. Esto nos hace crear esta ponencia sobre ciberseguridad. Nosotros estamos a favor del uso de las redes, a favor del uso de Internet, pero también estamos a favor de dar seguridad a los ciudadanos.

Usted hablaba de los delitos que empiezan a preocuparnos, y, efectivamente, los de menores son muy preocupantes. Tengo un ahijado de cuatros años al que hace unos días le pregunté qué quería de regalo de Reyes y me dijo que un móvil. Es decir, el uso de las tecnologías, de un móvil, de un iPad ya está generalizado. Lógicamente, los desafíos deben ser globales y las respuestas también, y esto no solo afecta a España, afecta a Europa y al mundo. Los delitos se mueven por el ciberespacio. Con el anterior compareciente hablábamos de guerras en el ciberespacio y ahora hablamos de delitos y de conductas punitivas en el ciberespacio.

A diferencia de los anteriores portavoces, no le voy a contar mi libro, lo que quiero es que usted, si puede, me responda a una serie de preguntas, aunque algunas ya las ha respondido, pero como las preparé ayer no sabía que lo iba a hacer antes de formulárselas. Lo que me interesa en esta ponencia es saber los criterios de los expertos. Usted es la experta y nosotros no lo somos en esta materia. ¿Cuenta la fiscalía con los medios humanos, materiales y presupuestarios necesarios para hacer frente al fenómeno de la cibercriminalidad, teniendo en cuenta que, además del hecho delictivo del que se está tratando, la investigación y la persecución son muy complicadas? Muchas veces nos enfrentamos aquí a la huella digital, es decir, en ocasiones no sabemos quién está detrás de esos delitos, con lo cual la investigación y la prueba a través de medios tecnológicos es muy complicado. Segunda pregunta. ¿Son suficientes los mecanismos, procedimientos y protocolos de actuación de la fiscalía en el marco de los distintos procedimientos judiciales que están establecidos en el ordenamiento jurídico español para la investigación y persecución de la criminalidad cibernética considerando su naturaleza esencialmente transnacional y las dificultades que plantea? Hemos visto como a lo mejor se comete el delito aquí pero es desde otro país.

Tanto el ministerio fiscal como las Fuerzas y Cuerpos de Seguridad del Estado están realizando un enorme esfuerzo para adaptarse al desafío que supone el crecimiento exponencial de cibercriminalidad, pero ¿cuáles son los problemas que se plantean, en su caso, en el desarrollo de procedimientos judiciales cuando se trata de admisibilidad de pruebas electrónicas o a evidencias digitales? Tanto en el marco de la Unión Europea como en el Consejo de Europa se está trabajando sobre el tema de la evidencia digital y electrónica. Dada la naturaleza eminentemente transnacional de la cibercriminalidad, ¿cuáles serían las medidas que se habrían de adoptar en materia de acceso, preservación y presentación de esas evidencias? ¿Son suficientes los mecanismos de cooperación existentes a nivel europeo e internacional en materia de cooperación policial y de asistencia judicial a la cibercriminalidad? ¿Considera que la fiscalía se encuentra capacitada para hacer frente a la comisión de delitos complejos desarrollados en el domino del ciberespacio, en el que los actores involucrados disponen de recursos ilimitados y dirigen sus actividades hacia la guerra económica, incluso hacia el sistema democrático, como hemos visto en algunos casos? ¿Cree compatible la necesidad de autorización judicial para la adopción de medidas de investigación que afectan a los derechos fundamentales con las diligencias de investigación penal del ministerio fiscal? ¿Considera que sería útil la autorización legislativa que permitiera proseguir una

cve: DSCG-12-CM-73

investigación fiscal, a pesar de requerir dichas autorizaciones judiciales? Ha hablado de pasada del agente encubierto. ¿Qué utilidad y qué reformas sugeriría en el régimen jurídico del agente encubierto informático? Y ahora que están de moda las criptomonedas, por desgracia, ¿qué medidas o diligencias de investigación deben regularse de cara a la investigación de ilícitos penales en los que se hayan empleado criptomonedas? ¿Ve usted posible una investigación preliminar del ministerio fiscal con la batería de medidas de investigación actualmente reguladas o considera que deben ser ampliadas para hacer frente a este nuevo tipo de amenazas? ¿Cómo cree usted que se está tratando el bien jurídico ciberseguridad en la normativa penal y procesal española? ¿Qué mejoras propondría usted en su tratamiento normativo, si las cree necesarias?

Por último —esto ya es un tema personal y político del Partido Popular—, nosotros creemos en la necesidad de una ciberreserva. ¿Cómo vería desde la fiscalía que España, la fiscalía y las Fuerzas y Cuerpos de Seguridad del Estado se pudieran dotar de voluntarios, de gente que tiene talento, que tiene conocimientos en el mundo del ciberespacio y que podrían poner esos conocimientos a disposición del Estado? Todo lo que nos diga para nosotros va a ser muy importante, tan importante que hoy me he traído a la portavoz de Justicia del Partido Popular para tomar nota por si tenemos que llevar a cabo alguna sugerencia. Decía el representante de Ciudadanos que había que apurarse, pues nosotros ya traemos a la portavoz de Justicia.

Muchísimas gracias.

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

La señora **FISCAL DE LA SALA COORDINADORA EN MATERIA DE CRIMINALIDAD INFORMÁTICA** (Tejada De la Fuente): Muchísimas gracias.

Son muchísimas las cuestiones planteadas y no sé de qué tiempo dispongo.

El señor **PRESIDENTE:** Diez minutos.

La señora **FISCAL DE LA SALA COORDINADORA EN MATERIA DE CRIMINALIDAD INFORMÁTICA** (Tejada De la Fuente): ¿Sí? **(Risas).** Voy a intentar contestar brevemente porque es prácticamente un estudio de todo en lo que estamos trabajando.

El señor Legarda planteaba el problema de la territorialidad. Efectivamente, es uno de los grandes problemas que tenemos en la lucha contra la ciberdelincuencia porque, además, los delincuentes —que no son tontos— se sirven de ello. Normalmente, cuando se prepara, por ejemplo, una estafa masiva frente a ciudadanos españoles, no se hace desde Madrid o desde Sevilla sino, por ejemplo, desde Bruselas. Y cuando ven que encima a Bruselas llegamos bien porque en el marco de la Unión Europea hay una cooperación reforzada y es relativamente fácil el trabajo entre autoridades policiales y judiciales, entonces se van a Ucrania para dificultarlo. Es un gran problema que está ahí y hay que luchar contra él, pero yo creo que hay que ver con optimismo lo que se está avanzando. Todas esas menciones que he hecho a la Convención de Budapest, a la legislación internacional, van en esa línea, es decir, es fundamental que seamos capaces de aproximar nuestras legislaciones lo más posible, que seamos capaces de tener unas herramientas comunes. ¿Que va a haber siempre países que están fuera? Sin lugar a dudas; sin lugar a dudas vamos a tener paraísos para los ciberdelincuentes, pero a eso tenemos que acostumbrarnos porque no ocurre solo en esta materia. Lo que hay que hacer es no perder de vista eso y centrarnos en lo que podemos hacer, y yo creo que se están haciendo avances importantes.

Les he hablado antes de la Convención de Budapest, que la han suscrito 53 países, casi todos los del Consejo de Europa. No hace falta que les diga que la Federación Rusa no ha suscrito la Convención de Budapest, pero sí lo han hecho países como Estados Unidos, Israel, Japón, Canadá y muchos iberoamericanos como Panamá, República Dominicana, Argentina acaba de aprobar la ley de incorporación a la Convención de Budapest, Chile… Todo eso es bueno porque quiere decir que con todos esos países vamos teniendo esa legislación común con la que ya podemos entendernos mejor. Todo esto son avances y hay que verlo así; yo siempre tiendo a ver la botella medio llena, no medio vacía, porque creo realmente que es la única forma de enfrentarse a los problemas. Es cierto que en algunos ámbitos se está empezando a jugar con otro planteamiento de lo que es la soberanía a partir de entender que a lo mejor un concepto excesivamente pegado al territorio dificultaría la cooperación necesaria en la lucha contra la ciberdelincuencia. Por ejemplo, una de las herramientas con las que se está trabajando en la Convención de Budapest es el acceso transfronterizo a datos informáticos, que nosotros ya lo tenemos en

cve: DSCG-12-CM-73

nuestra legislación. Esto quiere decir que si yo desde este sistema, desde este dispositivo, puedo acceder a información que está en la nube, porque puedo acceder directamente ya que es accesible desde este sistema, quizá no hay que recurrir a una medida de cooperación internacional sino que se puede hacer directamente. Se están barajando este tipo de conceptos que intentan superar los mecanismos clásicos de cooperación para hacer más ágil y más fácil la colaboración, partiendo de que cuando nos metemos en el ciberespacio no hay países.

Ha comentado también el problema de que estamos hablando de un derecho penal más de riesgo que de conductas que lesionan bienes jurídicos concretos. Tiene usted razón. En determinadas materias se está dando ese paso adelante, se está adelantando la barrera de protección, tipificando conductas que en realidad son conductas de riesgo. Por ejemplo, en la actual tipificación de los ataques a los sistemas de información ya se sanciona la mera posesión, adquisición o fabricación de herramientas aptas para cometer ataques informáticos, pero es porque el daño que ocasionaría ese ataque es tan serio que, a veces, hay que adelantar la barrera. Ahora se está siendo muy cuidadoso en esto, por lo menos el legislador español se ocupa mucho de cerrar todos los elementos de tipo penal para que el derecho penal se aplique solamente allá donde proceda aplicarlo. En esos delitos se exige que se demuestre que esas herramientas que se posee o que se han fabricado son para cometer un ataque informático, y eso le corresponde probarlo al fiscal, con lo cual se incorpora un elemento subjetivo que cierra el tipo penal y hace que no se aplique más que en los supuestos en los que sea estrictamente necesario.

El señor Salvador ha hablado de la especialización de las fiscalías y, efectivamente, está bien informado. Agradezco la referencia que ha hecho al trabajo que se está realizando en el área de especialización en criminalidad informática y comparto su opinión de que es un área que tiene que cuidarse y reforzarse porque cada vez tenemos más trabajo. Nosotros empezamos siendo cincuenta y dos, un fiscal por cada una de las fiscalías provinciales españoles y los dos que coordinábamos la red desde Madrid, y ya somos más de ciento cincuenta y no llegamos. Y eso que no intervenimos directamente en todos los asuntos, solo en los más complejos, en el resto intentamos de alguna manera coordinar. Hay que potenciar esto, pero también es cierto que hay que formar en estas tecnologías. La preparación de un especialista en ciberdelincuencia exige no solo conocimientos jurídicos sino también conocimientos técnicos que el operador jurídico no tiene porque no los hemos adquirido en nuestro currículum y que para nosotros son difíciles de adquirir porque nos son desconocidos. Esa formación básica en conocimientos técnicos básicos como qué es una IP, cómo funciona una wifi, cómo opera un correo electrónico, cómo se descarga una cabecera de un correo electrónico, etcétera, deberían tenerla todos los fiscales —con esto aprovecho para contestar a alguna de las otras preguntas— porque cada vez más la delincuencia se está moviendo a través de Internet. De acuerdo que tendremos que tener unas personas a la cabeza que sean las que vayan en la avanzadilla de esa preparación y continuamente mejorando sus conocimientos, pero el resto de los operadores jurídicos tienen que tener conocimientos suficientes.

Se refería también a la necesidad de que se vayan mejorando los sistemas de seguridad de la banca, etcétera. Efectivamente se está haciendo, es decir, las entidades bancarias cada vez mejoran más sus sistemas de seguridad. Si antes las claves bancarias se lograban sustraer aprovechando entradas irregulares en los dispositivos móviles, ahora hay medidas de seguridad reforzadas, la comunicación después de que se ha hecho la operación para que podamos darnos cuenta de que se ha hecho una operación con nuestras claves sin que la hayamos autorizado nosotros… Es decir, vamos avanzando, lo que pasa es que los delincuentes también y esta es una batalla a ver quién puede más. Nosotros intentamos mantener una colaboración muy directa con todas las entidades del sector privado que son foco de especial actuación por parte de los ciberdelincuentes. Nos hemos reunido varias veces con comisiones internas que tiene la banca de seguridad informática para trasladarles la necesidad de que denuncien los hechos, porque para poder actuar contra muchos de estos comportamientos y que haya una respuesta desde el Estado de derecho tiene que existir una previa denuncia. Al mismo tiempo nos vamos enterando de esos nuevos procedimientos que se están llevando a efecto para cometer las defraudaciones y vamos buscando medios para investigarlos, porque de eso es de lo que se trata, cómo investigamos estas nuevas formas de comisión que van surgiendo al hilo de la evolución tecnológica. Es nuestra pelea de cada día.

Ha hecho usted también algún comentario a propósito de las conductas injuriosas o difamatorias respecto de los funcionarios públicos. Comparto plenamente su visión, el problema es que la red hace llegar comentarios de todo tipo a todo el mundo y efectivamente se puede atentar muy seriamente contra el honor, la dignidad y el respeto a las personas y son hechos que deben ser sancionados. En relación con

cve: DSCG-12-CM-73

esto únicamente querría precisar una cosa que no sé si queda suficientemente clara, y es que cuando se trata de imputaciones de carácter injurioso o calumnioso realizadas en relación con autoridades públicas en el ejercicio de sus funciones y por hechos concernientes a sus cargos, la persecución es de oficio, en ese caso no sería necesaria la querella del afectado sino que podría actuar la fiscalía de oficio o la policía de oficio porque ahí se protege otro interés; aparte del específico, el honor de la víctima, se defiende también el respeto debido al ejercicio de esa función pública. Agradezco su apoyo a la labor que está haciendo la fiscalía. Estamos trabajando todo lo que podemos por actuar frente a esta forma de delincuencia.

El señor Comorera hablaba básicamente de formación. Comparto plenamente las afirmaciones que ha realizado. Efectivamente, tiene buena información. Nosotros estamos intentando plantear la formación en dos niveles, ya lo he explicado. Una formación muy especializada, constante y permanente para los que usted llama delegados, que es en definitiva la red a la que yo me he referido, y aquí estamos encontrando colaboración de escuelas técnicas de ingeniería o de telecomunicaciones porque es una formación muy específica, y al mismo tiempo organizar actividades de formación general para todos los fiscales a otro nivel. A eso me refería cuando hablaba de la formación a dos niveles. Lo que pasa es que los recursos económicos con los que contamos son muy escasos, lo tengo que decir. En el plan de formación del año próximo creo recordar que se han organizado cinco o seis cursos de carácter general para todos los fiscales que se refieren específicamente a ciberdelincuencia, a razón de 35 o 40 alumnos por curso hay que sacar la cuenta, y somos 2500 fiscales. A eso me refería antes al decir que hay que ser mucho más ambiciosos. De hecho, les diré —y creo que este es un buen lugar para decirlo— que cuando desde la fiscalía trabajamos en los planes derivados de la Estrategia Nacional de Ciberseguridad se aprobó un proyecto según el cual había una cantidad de dinero —no me pregunten cuánto porque no me acuerdo— destinada precisamente a la formación de fiscales y de jueces, de operadores jurídicos, en materia de ciberdelincuencia, y la verdad es que no se ha concretado finalmente. Yo creo que esta es un área en la que hay que apostar muy seriamente para la formación.

Aunque no me lo han preguntado, quiero referirme a la formación de las Fuerzas y Cuerpos de Seguridad del Estado porque me parece un tema extraordinariamente serio. Son unidades que están haciendo una labor extraordinaria y para nosotros son fundamentales. Yo se lo explico con toda la sinceridad del mundo, nosotros sabemos de derecho, pero no de tecnología. Entrar en las redes y encontrar las pruebas en las redes lo tienen que hacer ellos y luego nosotros valorarlo. Sin embargo, sus cuadros son muy pequeños, tienen muy poca gente. El tema, por ejemplo, de los laboratorios de policía científica y criminalística también es muy preocupante, están muy poco dotados y casi todas las investigaciones, no ya de ciberdelitos sino de cualquier delito, necesitan un análisis de dispositivo electrónico. Antes lo comentaba con uno de ustedes en *petit comité*, el asunto de Diana Kerr, por ejemplo, no tiene nada que ver con las tecnologías, es una mujer que desapareció y que no sabemos dónde está, pero toda la investigación que se ha hecho está sobre su móvil, con lo cual hay muchos hechos delictivos en los que, aunque en principio son ajenos al uso de las herramientas tecnológicas, la prueba es electrónica; ahí hay que invertir mucho esfuerzo porque es la base de una investigación criminal adecuada.

Se refería también usted a las estafas. Efectivamente, otro de los problemas es la investigación de esas estafas en las que hay cientos de perjudicados distribuidos por todo el territorio nacional que se creen una oferta de un viaje por 400 euros a las islas no sé qué quince días en un hotel de lujo. De esas tenemos muchas y no tenemos más remedio, si queremos actuar frente a esas conductas, que unir en un único procedimiento toda esa miriada de pequeños perjudicados. Eso supone un trabajo inmenso. Lo estamos haciendo desde la fiscalía, a través de nuestra red de fiscales vamos localizando a estos perjudicados para unirlos en un procedimiento común, con la importantísima colaboración que nos prestan las Fuerzas y Cuerpos de Seguridad del Estado.

Me hablaba también de los delitos de odio. Cada uno de estos temas daría para muchísimo. ¿Qué criterios seguimos? Los legales, no puedo contestar de otra forma, y los que van siendo fijados por los órganos jurisdiccionales. El Tribunal Supremo y el Tribunal Constitucional se han pronunciado ya mucho sobre los delitos de odio. Son figuras delictivas complicadas, igual que pueden serlo los delitos contra el honor, por ejemplo, el enaltecimiento del terrorismo o la humillación de víctimas, porque entran en colisión derechos fundamentales en los dos casos, libertad de expresión por un lado y derecho a la intimidad y a la privacidad por otro. Encontrar el punto justo y a partir de qué momento el hecho ya es constitutivo de delito porque rebasa los límites de la libertad de expresión supone un estudio muy profundo del contenido,

cve: DSCG-12-CM-73

no solo de la frase concreta sino en su contexto, cómo se dice, de qué manera, e intentar combinar en cada supuesto concreto lo que ampara la libertad de expresión y lo que excede de ella.

El señor Luena me ha preguntado si hemos hecho algo en la ley de seguridad de las redes y de los sistemas informáticos. Muy poco. Hemos tenido interés en ese tema desde el primer momento y nuestro interés es el que les he comentado. Es una oportunidad de oro —porque los ataques informáticos, insisto, no se están denunciando— para que, como la autoridad pública, la que sea, la destinataria última de esas notificaciones de incidentes de seguridad, va a tener conocimiento de esos hechos, cuando esos hechos sean constitutivos de delito se los traslade a la fiscalía, al órgano judicial, a las Fuerzas y Cuerpos de Seguridad del Estado, me da igual, pero a los órganos de la jurisdicción penal. En realidad, es una obligación legal que ya existe, lo dice creo que el artículo 262 de la Ley de Enjuiciamiento Criminal, del siglo XIX, lo que pasa es que a veces hay que recordar esto. Es importante, además, por lo que he dicho, porque creo que la única forma de responder de forma seria a los ataques informáticos es combinando la prevención con el castigo, lo digo sinceramente. Hay que romper ese sentimiento de impunidad que hay en la Red, en la que parece que todo vale. Hay que ser capaces de actuar frente a esas conductas y por eso me parece importante.

Ha hablado también de la formación de fiscales y me remito a lo que ya he dicho anteriormente por no repetirme. Preguntaba si tenemos datos. Tenemos datos estadísticos concretos pero no completos —ya lo he dicho—, porque recabar esa información nos está resultando extraordinariamente trabajoso. A este respecto podría hablar de otro problema, y es que nuestras aplicaciones informáticas no están preparadas para recoger bien este tipo de actividades delictivas. Necesitaríamos unas aplicaciones informáticas mucho más precisas. No obstante, con un trabajo muy artesanal de los fiscales, estamos obteniendo datos desde el año 2011, los tienen en nuestras memorias. Ahora mismo me resulta imposible hacer la evolución porque no tengo los datos en la cabeza, pero las estafas son los hechos que más se denuncian todos los años, no los que más se cometen, y están subiendo mucho en las últimas memorias —se lo digo porque me lo preguntaba— todas las denuncias por delitos contra la intimidad, la libertad y seguridad, acosos, amenazas, etcétera. Ese tipo de conductas están subiendo mucho y también estamos teniendo una intervención cada vez mayor en los temas relacionados con los delitos de odio, en buena medida porque existe una mayor colaboración ciudadana en esta materia.

En cuanto al Centro Criptológico Nacional, tenemos unas buenas relaciones, pero normalmente la transmisión de información que puede tener carácter delictivo del Centro Criptológico Nacional se hace directamente a Fuerzas y Cuerpos de Seguridad del Estado, no a la fiscalía; en realidad, un hecho delictivo se puede denunciar ante Fuerzas y Cuerpos de Seguridad del Estado, policía judicial, fiscalía y jueces. Si es ante el centro criptológico, no pasa nada, pero quería hacer esa precisión. Respecto a los datos concretos por los que me preguntan, no tengo ninguno. Sobre yihadismo ya he dicho que no es un tema de nuestra fiscalía sino de la fiscalía de la Audiencia Nacional, que es la que lleva específicamente temas en materia de terrorismo. Lo que sí que les quiero decir es que la fiscalía actúa como un bloque porque somos uno. A veces nos llegan a nosotros denuncias como ciberdelincuencia que son de terrorismo y lo que hacemos es, en la primera investigación, en la puramente tecnológica, intentar averiguar quién ha sido y dónde ha sido y lo pasamos a nuestros compañeros de la Audiencia Nacional para que ellos sigan su labor desde su especialidad en la lucha contra el terrorismo.

En cuanto a cooperación con operadores de comunicación y proveedores de servicio, estamos trabajando todo lo que podemos en este sentido. Tenemos contactos buenos para retirada de contenidos, para preservación de contenidos que necesitamos después para utilizarlos como medios de prueba, pero ahí queda camino por andar. Lo tengo aquí apuntado; si quieren ustedes que venga cada poco tiempo, estaré encantadísima, me sentiría muy honrada.

Ha planteado también el tema de las informaciones relacionadas con el supuesto espionaje o desinformación por parte de determinados países que pueden operar sobre acontecimientos que ocurran en nuestro país. No todo lo que se hace en la Red es malo o es delito. Hay muchas cosas que se hacen en la Red que son reprobables, que no son correctas, pero que no están tipificadas como delito. Para que un hecho pueda perseguirse como delito es necesario que esté tipificado específicamente como delito y que reúna los requisitos que exige un tipo penal. Por ejemplo, desinformar para alterar los valores y las cotizaciones del mercado de valores es delito, es un delito contra el mercado y los consumidores; desinformar y decir que ha ocurrido un atentado terrorista para que salga toda la policía, los bomberos y las ambulancias también es un delito, es un delito de desórdenes públicos. Tendría que ver específicamente

cve: DSCG-12-CM-73

de qué estamos hablando para saber si es encajable en algún tipo penal concreto y determinado. No sé si le he respondido a lo que me ha preguntado.

Quiero agradecerle al Grupo Popular sus preguntas y comentarle que en la fiscalía hacemos lo que podemos; tenemos los medios que tenemos y con esos medios estamos volcando todo el esfuerzo, toda la ilusión y todo el empeño por salir adelante. Evidentemente, hay cosas que podrían estar mejor y que podríamos tener mayores medios personales y materiales para investigar pero, como decía antes otro de los portavoces, nuestras herramientas informáticas son escasas y la formación tiene los problemas que le he dicho.

En cuanto a las capacidades de actuación de la fiscalía y de, por ejemplo, todo eso que comentaba usted a propósito de que la fiscalía pueda seguir más adelante en las investigaciones, lo cierto es que la Ley de enjuiciamiento que tenemos es la que tenemos. Es decir, nosotros ahora mismo iniciamos una investigación, de entre las muchas que iniciamos en relación con esta materia pero, como casi siempre nos encontramos con que para acceder a la información necesitamos autorización judicial, resulta que al ir a pedirle al juez dicha autorización para acceder a esa información —porque si no podemos continuar con la investigación—, necesariamente tenemos que judicializar el procedimiento y, por tanto, perdemos la investigación. Efectivamente, sería posible que el fiscal reclamara esa información al juez y, una vez la hubiéramos obtenido, podríamos seguir adelante con nuestra investigación pero con la información que nos ha facilitado la intervención del juez y sin que eso supusiera perder nosotros la dirección. Sin embargo, en ese caso, estaríamos hablando de otro modelo que no es el que tenemos ahora, sería un modelo que apostaría por la investigación en manos del fiscal y que yo creo que en esta materia, en la lucha contra la ciberdelincuencia, aportaría mucho de valor. Pero es un debate muchísimo más amplio que, desde luego aquí, no me siento siquiera capaz de dibujarlo.

Se refería usted a los mecanismos de cooperación internacional y a la obtención de evidencias y le tengo que decir que se está trabajando en todo ello. Como decía anteriormente a propósito de la convención de Budapest, uno de los trabajos en los que estamos volcados profundamente es facilitar la obtención de evidencias más allá de las fronteras de los Estados, intentando que no sea imprescindible acudir a mecanismos de cooperación, que son mucho más lentos y costosos. Es una materia que exige de mucho trabajo, y además de mucho trabajo a nivel internacional, es decir, no basta con lo que nosotros hagamos, si bien se está trabajando en esa línea.

Asimismo, me planteaba dos cosas muy, muy concretas. Una de ellas es el tema del agente encubierto y la otra el tema de las criptomaneras. Discúlpenme, pero son muchas preguntas y me es imposible contestar a todas.

En cuanto al agente encubierto, efectivamente, supone un gran avance la regulación del agente encubierto *online*. Como ya he dicho aquí, es una figura que se incorporó en la reforma de 2015 y es algo que está siendo imitado por otros países porque, aunque ya existía una figura de agente encubierto físico, la investigación en la red presenta unas peculiaridades específicas. Novedades al respecto solo se me ocurre una; La ley dice que agente encubierto solo puede ser un funcionario de la Policía judicial designado por el juez y controlado en su actuación por este y nosotros nos estamos planteando si quizá en algunas ocasiones no sería bueno poder contar para ello con particulares porque a veces esas operaciones encubiertas se desarrollan en foros muy específicos donde se hablan lenguas específicas —y estoy pensando en terrorismo, por ejemplo— o con un lenguaje muy críptico, muy de ellos, por lo que en ocasiones, para un agente que no está normalmente en esos foros, resulta difícil encubrir quién es. Tal vez habría que valorar eso.

El problema de las criptomaneras, y termino con ello, trasciende mucho al problema de la lucha contra la ciberdelincuencia. Es un fenómeno que se está produciendo, que está teniendo una incidencia y que hoy por hoy está sin regular, es decir, ni es legal ni ilegal, es alegal, en definitiva, no hay regulación. Es cierto que nos estamos encontrando ya con algunos problemas prácticos, concretamente, ha habido algunos operaciones en las que hemos incautado *bitcoins*. ¿Qué hacemos con los *bitcoins*? Porque la Ley de Enjuiciamiento Criminal detalla lo que hay que hacer en el caso de incautación de dinero, en el caso de bienes muebles, en el caso de administración de empresas, pero sobre criptomaneras no hay nada. Habría que regular si hay que trasladarlo a moneda de curso legal y depositarlo en un banco, si hay que crear monederos digitales controlados por los órganos de la Administración para hacer el depósito de esas criptomonedas. Este es un tema que se nos está planteando y que está sin regular. Sería bueno empezar a pensar en que los intermediarios en las operaciones de criptomonedas deberían tener ciertas

cve: DSCG-12-CM-73

obligaciones establecidas por la ley sobre quiénes hacen las operaciones o la obligación de identificar a quienes llevan a efecto esas operaciones, los movimientos económicos, etcétera. Podría ser un principio.

Lo siento, pero no puedo extenderme más, aunque los temas dan para mucho.

El señor **PRESIDENTE:** Muchísimas gracias.

Tengo que abrir un segundo turno. ¿Señor Legarda? **(Denegación).** ¿Señor Salvador? Tiene la palabra.

El señor **SALVADOR GARCÍA:** Intervengo muy rápidamente, señor presidente.

En primer lugar, vuelvo a ratificarme en los agradecimientos. Quiero decir que esta Comisión es de seguridad nacional y estamos hablando de ciberdelincuencia y ciberdelitos, y creo que —lo digo por la portavoz del Grupo Popular— no hace falta ser expertos, pero sí por lo menos tener una visión. No se entendería que, por ejemplo, en la Comisión de Asuntos Exteriores no se tuviera una visión clara de lo que es el mundo, de los conflictos regionales, de cuáles son los actores para poder actuar y proponer cosas. En esta Comisión nos sucede lo mismo, o somos capaces nosotros mismos de interpretar el mundo en el que vivimos, las complejidades que tiene y este tipo de delitos y acontecimientos, o difícilmente esta ponencia nos podrá servir de algo. Lo digo como un alegato y porque no quiero que se lleve usted la imagen de que todos los que nos sentamos en este banco venimos aquí como si estudiáramos primero de Primaria a ver lo que nos cuenta y aprendiéramos un poquito en este campo. Tenemos que saber un poquito y también exponerse cuáles son las cosas que estamos viendo para que usted nos pueda dar la respuesta técnica de la persona que está en el día a día en esta materia.

Para terminar, no me refería tanto a la banca, que ha invertido muchísimo dinero y es probablemente la más segura en todo este tema del comercio electrónico, como sí a tener una red confiable, porque yo, por ejemplo, utilizo un banco con mi tarjeta y sé que normalmente eso está bastante garantizado y que no habrá ningún problema, pero cuando voy a sacar un billete de tren por Internet me piden los datos de la tarjeta de crédito, igual que para otras muchas cosas. Si yo tengo la sensación de que la red es confiable, porque estoy utilizando servicios que son confiables, también puedo entender que toda la red y todos los servicios que me están ofreciendo y en los me piden también los datos de una tarjeta también pueden ser confiables porque todos utilizan el mismo tipo de encriptamiento, de protección de la información, etcétera, y sabemos que eso no es verdad. Eso es lo que quería manifestar no tanto sobre la banca, que sí está muy protegida y muy blindada, como sobre la confianza de los ciudadanos en ese comercio electrónico porque, si no, ahí sí entramos en un problema muy grande porque hoy se están enfocando muchos modelos de negocio a la red, y ahí la confianza es el elemento fundamental para poder operar adecuadamente.

Para terminar con lo que empezaba, estoy de acuerdo con lo que usted está diciendo, que todos los fiscales, a fin de cuentas, y todos tenemos que comprender el mundo en el que nos estamos desenvolviendo y hacia dónde van los tipos de delitos, independientemente de que ustedes sean los fiscales especializados a quienes tenemos que reforzar en medios. También estamos de acuerdo con lo que ha dicho sobre la policía científica y la carencia de medios, porque yo he visitado varios laboratorios de policía científica y he visto que hacen un trabajo impresionante, pero a veces parece un poco rudimentario y podrían tener muchas más facilidades a la hora de actuar. Como antes le he dicho, le apoyo en todo lo que usted necesite.

Muchas gracias.

El señor **PRESIDENTE:** Señor Comorera.

El señor **COMORERA ESTARELLAS:** Intervendré brevemente. Solo para agradecer una vez más las respuestas extensas que nos ha dado sobre las preguntas que le hemos formulado e incidir en lo mismo que comentaba el señor Salvador, sobre todo en el tema de la policía científica. Antes de ser senador lo he sufrido bastante. Ha habido informes de policía científica que nos han tardado más de un año cuando los plazos de instrucción de los procedimientos están establecidos en seis meses y, en un informe bastante simple, esa misma policía científica te responde directamente que por cuestión de falta de medios antes de un año no tendrá ese informe solicitado

Nos quedamos con el tema de la formación y de los medios; intentaremos ponerle el remedio que sea posible.

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

Señor Luena.

cve: DSCG-12-CM-73

El señor **LUENA LÓPEZ:** Deseo agradecer a la señora Tejada de la Fuente el trabajo que ha hecho aquí hoy, porque ha sido trabajo; le vendrá muy bien a esta Comisión y a la ponencia que tenemos. Desde luego será muy valioso y lo tendremos muy en cuenta.

El señor **PRESIDENTE:** Gracias, señor Luena.
Señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Muchas gracias.
Lógicamente, deseo agradecer las respuestas. Nos llevamos muchísimas ideas para los que no tenemos tantos conocimientos y hacemos las reflexiones previas en los despachos. También deseo dar las gracias al presidente. Creo que estamos teniendo unas sesiones de la Comisión de mucho nivel, y ya la prensa está siguiéndonos más a menudo. Así que le agradezco mucho el interés que ha puesto el presidente.
Ya que es la última intervención les deseo a todos Feliz Navidad y Felices Fiestas.

El señor **PRESIDENTE:** Voy a despedir a la fiscal y cierro esta Comisión.
Deseo, puesto que esta es nuestra última sesión, Feliz Navidad a los creyentes; feliz solsticio de invierno a los no creyentes y Feliz Año a todos.
Muchas gracias.
Se levanta la sesión.

Eran las dos y cuarenta y cinco minutos de la tarde.

cve: DSCG-12-CM-73