DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 83 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 14

celebrada el miércoles 7 de marzo de 2018 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

Proposiciones no de ley:

---

cve: DSCG-12-CM-83

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

PROPOSICIONES NO DE LEY:

— SOBRE LA POLÍTICA DE DEFENSA ORIENTADA A LA PREVENCIÓN DE ATAQUES BIOTERRORISTAS CON VIRUS DE LA VIRUELA. PRESENTADA POR EL GRUPO PARLAMENTARIO MIXTO. (Número de expediente del Congreso de los Diputados 161/001928 y número de expediente del Senado 663/000035).

El señor **PRESIDENTE:** Buenas tardes. Vamos a empezar la reunión.

Tenemos hoy el debate y votación de cuatro proposiciones no de ley, lo cual nos va a exigir ser relativamente cicateros en el uso de los tiempos. En principio, como sus señorías saben, el ponente de la proposición tendrá diez minutos, el enmendante cinco y cada uno de los grupos tres.

La primera de las proposiciones es la que se refiere a la política de defensa orientada a la prevención de ataques bioterroristas con virus de la viruela, de la que es autor el Grupo Parlamentario Mixto, y tendrá la bondad de explicárnosla el señor Xuclà.

El señor **XUCLÀ I COSTA:** Muchas gracias, señor presidente.

Señorías, ya fue en el lejano mes de mayo del año 2015 cuando quien les habla tuvo la oportunidad de formular en el Pleno del Congreso de los Diputados una interpelación al ministro de Defensa de aquel momento, don Pedro Morenés, planteando la necesidad de que la Estrategia de Seguridad Nacional incorporara un enfoque más activo con respecto al reto del bioterrorismo. A aquella interpelación siguió una moción que fue aprobada casi por unanimidad del Pleno del Congreso de los Diputados —305 votos a favor y una abstención—, y el Congreso de los Diputados, su Pleno, mandataba al Gobierno a proceder a una revisión y actualización de la estrategia con respecto a bioseguridad y también a una revisión y actualización del inventario de medios y equipos, medicamentos y vacunas a disposición del Gobierno para hacer frente a las eventuales amenazas biológicas para la seguridad, así como a una revisión de los protocolos y mecanismos de colaboración existentes.

Señorías, esta Comisión Mixta está dedicando tiempo y esfuerzos muy apropiadamente al reto de la ciberseguridad, pero, conjuntamente con esta, el bioterrorismo es uno de los grandes retos para nuestra seguridad global. El bioterrorismo es el uso intencionado de un patógeno o producto biológico con el objetivo de producir daño a personas, animales, plantas u otros organismos para influir sobre la conducta de los Gobiernos o intimidar a la población civil. Se utilizan virus, bacterias u otros gérmenes en laboratorios para aumentar su capacidad de dispersión o ser más dañinos. Los expertos consideran que son más letales y baratos que los químicos y más difíciles de detectar, y uno de los más peligrosos es la viruela.

En los países desarrollados este es un riesgo real, que se acrecienta con la globalización y las tensiones internacionales. Ante esta creciente amenaza, países como Francia, Alemania, Dinamarca, Estados Unidos y Canadá han afrontado una estrategia integral para dar respuesta inmediata en caso de ataque bioterrorista. No era el caso en el año 2015, cuando quien les habla formuló la interpelación al ministro de Defensa de aquel momento. Desde entonces, en los posteriores informes sobre la Estrategia de Seguridad Nacional se han incorporado algunos elementos sobre bioterrorismo y bioseguridad, pero con esta iniciativa queremos dar un nuevo impulso a las políticas activas en materia de bioseguridad. Vemos que se han presentado enmiendas por parte del Grupo Popular y el Grupo Socialista que básicamente vienen a apoyar la iniciativa del Partit Demòcrata y creo que será muy posible un acuerdo con respecto a ellas.

Nosotros proponemos incorporar en el método de trabajo del Consejo de Seguridad Nacional el enfoque de una política integral e interministerial de la lucha contra la amenaza bioterrorista. Proponemos incorporar en el informe anual de seguridad nacional una rúbrica —actualmente no existe— dedicada a las políticas de lucha contra el bioterrorismo. Proponemos elaborar un informe anual sobre las políticas de lucha y prevención contra la amenaza bioterrorista, presentar en el plazo de tres meses —y saludo que esta sea una iniciativa que apoyan las enmiendas del Grupo Popular y del Grupo Socialista— el primer informe ante esta Comisión Mixta de Seguridad Nacional incorporando los avances realizados desde la aprobación de aquella proposición del 26 de mayo de 2015, y revisar y actualizar el inventario de que dispone el Gobierno de medicamentos, equipos y vacunas para hacer frente a la amenaza del bioterrorismo, especialmente por el virus de la viruela. Sus señorías saben que la viruela fue fulminada

cve: DSCG-12-CM-83

como riesgo hace muchos años y que cualquier joven de menos de treinta y cinco años no ha sido vacunado contra ella, pero también saben bien que Estados Unidos o la Federación Rusa retienen y mantienen la cepa de la viruela, la cual —no soy nada alarmista, hay expertos que podrían comparecer en esta Comisión e ilustrar al respecto— está en el mercado negro de las armas bioquímicas. Por eso, en 2003, durante el segundo Gobierno Aznar, se produjo una compra de dos millones de efectivos de vacunas de la viruela, especialmente pensada para personal con alto riesgo, ejército, policía, servidores públicos, funcionarios públicos, aunque desde entonces no se ha renovado ese stock dedicado a las viruelas. No se trata de hacer reproches sobre el pasado, pero creo que han transcurrido muchos años y es evidente que la innovación tecnológica permite en estos momentos hacer frente a la amenaza bioterrorista y, concretamente, a esta del virus de la viruela. En quinto lugar, señorías, proponemos elaborar un plan de actuación sobre la amenaza del bioterrorismo en el que se incluyan métodos de detección y reconocimiento temprano de las personas infectadas, la adopción de medidas urgentes de protección física y de asistencia a la población y una evaluación de las consecuencias de los riesgos para la población, con el objetivo de tener una preparación y respuesta inmediata en caso de atentado bioterrorista.

Con esto termino, señor presidente; no agoto los diez minutos. Insisto en que agradezco al Grupo Popular y al Grupo Socialista las enmiendas, porque creo que, en términos generales, avalan la propuesta del Partit Demòcrata, y a partir de ellas tenemos la mejor predisposición para llegar a un acuerdo.

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

Por el Grupo Socialista, tiene la palabra la señora Botella.

La señora **BOTELLA GÓMEZ:** Gracias, señor presidente.

Efectivamente, señorías, estudiada la propuesta del Grupo Parlamentario Mixto, nuestro grupo valora positivamente esta iniciativa de lucha contra las amenazas que pueden suponer las armas de destrucción masiva, porque, en definitiva, aunque la propuesta se centra específicamente en amenazas de carácter bioterrorista y específicamente en el virus de la viruela, consideramos que debe orientarse hacia un enfoque global, lo que, de hecho, ya se consideró en la moción consecuencia de interpelación de 2015, aprobada por unanimidad en el Pleno del Congreso, una iniciativa que hacía fuerza al hablar de armas de destrucción masiva NBQR, termino empleado tanto en la Estrategia de Seguridad Nacional de 2013 como en la de 2017. Por eso, el sentido de la nuestra enmienda iría por esa elevación, para poder hacer frente a una amenaza mucho más global, aunque después se pueda hacer una especial consideración de algún agente biológico que se entienda pertinente.

Nos llama la atención que en 2018, prácticamente tres años después de aprobarse aquella moción por unanimidad en el Pleno del Congreso de los Diputados, volvamos a tener que debatir sobre esta iniciativa, cuando ha mediado ya un informe de seguridad nacional de 2016 y una actualización con la Estrategia de Seguridad Nacional de 2017, que, por cierto, hace menos mención e hincapié en este tema sobre armas de destrucción masiva que la de 2013. En ese sentido, nos preocupa que en una cuestión tan sensible para todos, y me consta que también para el Gobierno, se haya podido soslayar el impulso que desde el Congreso claramente se pidió al Ejecutivo. Creo que obedece a ese cierto autismo en el que está instalado el Gobierno del Partido Popular en los últimos años, que vive en paralelo a la Cámara. No es baladí una iniciativa de estas características y en su momento se llegó a un acuerdo muy completo por parte del Congreso de los Diputados, y, sin embargo, ahora tenemos que volver a plantearlo.

Finalmente, me gustaría hacer hincapié en que, en los términos en que nosotros hemos presentado la enmienda, se trata de hacer frente a las amenazas NBQR más completas. También quiero hacer hincapié en la coordinación interministerial que una amenaza como esta implica, así como en el aspecto preventivo y en la respuesta. La enmienda del Grupo Popular hace referencia en su último punto a un plan nacional de biocustodia que nos parece interesante, como lo es también la capacidad de respuesta, con todo lo que ello supone de cara a la sociedad. Asimismo, nos preocupa todo lo referido a protocolos, tanto en los aspectos de comunicación como de bioseguridad, capacidad de respuesta y centros donde han de instalarse los sistemas de control, aislamiento, etcétera.

Sintetizando, manifestamos nuestro apoyo a esta iniciativa y esperamos que a lo largo de esta sesión podamos concentrar los puntos de acuerdo y lograr una postura común.

Muchas gracias. **(Aplausos).**

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

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

cve: DSCG-12-CM-83

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

Para este Gobierno y el Grupo Popular la importancia de la prevención en terrorismo y bioterrorismo es máxima. Los eventos relativos al ébola recientemente acaecidos en África, que se han saldado con más de mil muertos, han puesto de manifiesto el riesgo que supone la aparición y evolución de patógenos en el medio ambiente y el impacto que pueden tener sobre la población. Y la población española, al igual que la mundial, es muy susceptible frente a la infección de la viruela, que, como decía el portavoz del Grupo Mixto, tiene una alta virulencia, una rápida transmisión por aire y una tardía detección, lo que complica su contención. Como todos saben, en España está erradicada desde 1980 y ya pocos conocemos a personas que tengan puestas la vacuna. Antes de empezar esta reunión hablábamos de los que llevan la marca en el brazo, y pocos son los miembros de la Comisión que la tienen. Por tanto, algunos no dispondríamos en este momento de una prevención así.

Actualmente España cuenta con un stock de dos millones de dosis dependientes del Ministerio de Sanidad y 48 800 dosis dependientes del Ministerio de Defensa, que se encarga de su custodia. Como decía el portavoz del Grupo Mixto, las vacunas son el modo más eficaz y barato de protección y la Unión Europea recomienda a todos los Estados prepararse ante un posible ataque químico o biológico, al igual que la propia OMS. Y aquí tengo que recordar a nuestra diputada Beatriz Rodríguez-Salmones, portavoz de Defensa en aquel momento y quien defendió la postura a favor del Grupo Popular. Y me gustaría señalar que no es dejadez del Gobierno. Creo que la señora Botella debe desconocer que en el año 2015 hubo unas elecciones que se convocaron en el mes de julio y que después hubo otras elecciones y un Gobierno que tomó posesión a finales de 2016, de manera que hace un año y tres meses que estamos en el Gobierno.

Sin lugar a dudas, aplaudimos la proposición no de ley, aunque hemos presentado una enmienda. En el primer punto se impulsa en el Consejo de Seguridad Nacional como método de trabajo el enfoque de una política de carácter interministerial e integral para tratar la amenaza con armas de destrucción masiva nucleares, químicas y biológicas, al tiempo que se prevé la creación de un comité especializado contra la proliferación de este tipo de armas, lo que completará y hará más efectiva esa acción integrada y coordinada por el Estado. El informe anual de seguridad nacional ya incluye un apartado específico contra la lucha de la proliferación de ADM a manos de actores no estatales, en particular, terroristas. Sin embargo, dada la magnitud de la amenaza, resulta conveniente que se reseñe de forma específica. Por eso estamos a favor de ese apartado y hemos presentado una enmienda. Se pretende promover el cumplimiento del Plan nacional de acción para la completa aplicación de la Resolución 1540 de Naciones Unidas y la elaboración de un informe sobre las medidas adoptadas para la prevención. En definitiva, en cumplimiento de esta Resolución 1540 contra la proliferación de armas biológicas, químicas y nucleares a manos de actores no estatales, en particular, terroristas, se insta a presentar en el plazo de tres meses el primer informe ante la Comisión Mixta de Seguridad Nacional con los avances realizados desde la aprobación del Plan nacional de acción por el Consejo de Seguridad el 24 de abril de 2015. Desde el Grupo Popular proponemos que el Gobierno presente en tres meses este informe ante la Comisión Mixta. El cuarto punto insta a revisar y actualizar el inventario del que dispone el Gobierno de medicamentos, equipos y vacunas para hacer frente a las amenazas del bioterrorismo, especialmente por el virus de la viruela. Reino Unido, Francia, Alemania ya lo están haciendo y el Gobierno español también está a favor de ello. Por último, se prevé la presentación de un plan nacional de biocustodia en el Consejo de Seguridad Nacional.

Esta es la enmienda que presentamos, y, por lo que he podido hablar con el portavoz proponente, espero que podamos llegar a un acuerdo y lograr una transaccional entre los dos grupos.

Muchas gracias.

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

Entramos en el turno de fijación de posiciones. Por tiempo de tres minutos, por el Grupo Ciudadanos tiene la palabra el señor Gutiérrez.

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

Nos parece que el debate sobre los diferentes vectores que acaban conformando una estrategia de defensa NBQR es muy importante. Apreciamos la iniciativa que trae el señor Xuclà, aunque nos parece limitada y sesgada. Vamos a votar a favor porque estamos de acuerdo, pero nos gustaría que el debate fuese un poco más amplio. No entendemos esta limitación o sesgo sobre el virus de la viruela, que, evidentemente, es un vector potencialmente peligroso, pero como otros muchos, por ejemplo, el ántrax. Y, sobre todo, es que hay otros vectores que no tienen que ver con el riesgo bacteriológico, sino con el

cve: DSCG-12-CM-83

riesgo nuclear, radiológico o incluso químico que hacen que necesitemos una protección adecuada, y a nosotros nos gustaría llevar el debate ahí, el debate sobre la formación de nuestras fuerzas y cuerpos de seguridad, que son los primeros que van a actuar en el caso de que exista una crisis de este tipo y respecto de los que entendemos que la formación no es adecuada. No hay una escuela de formación y sí diferentes grupos NRBQ en las diferentes fuerzas de seguridad del Estado, incluso de las propias comunidades autónomas, bomberos de ayuntamientos, policías locales y unidades como el Samur. Consideramos que no habría buena coordinación si en algún momento hubiese un riesgo de este estilo. No tenemos unas infraestructuras adecuadas para contener este tipo de ataques, y la prueba la tuvimos en 2014, cuando la crisis del ébola, cuando un hospital público como el Carlos III, en Madrid, tuvo que habilitarse con muchísima premura y creo que con muchísimo riesgo, primero, para los propios trabajadores del centro y también para el resto de la población. Nos parece que no se ha hecho ningún debate de este estilo, nos parece que el Gobierno no ha tomado ninguna medida, no se ha identificado, no tenemos un centro capaz de alojar a las víctimas que pudieran ser infectadas o atacadas por cualquiera de los vectores anteriores, y nos parece que ese es el debate de fondo, más allá de si se deben actualizar —por supuesto que sí— las vacunas o los antirretrovirales para dar contención a este tipo de crisis. Por eso, más que al Gobierno, instamos en este caso a la propia Comisión para que hagamos un debate sereno sobre todo el riesgo RNBQ, sobre cuál es la formación que deben tener nuestras fuerzas y cuerpos de seguridad y sobre cuáles deben ser las instalaciones. Nosotros consideramos que debería haber una instalación nacional, con expertos de verdad e infraestructura adecuada, capaz de controlar este tipo de crisis.

En todo caso, valoramos positivamente la iniciativa que presenta el señor Xuclà, como he dicho antes, y votaremos a favor. Pero queremos poner sobre la mesa que creemos que el debate debe ir más allá de cuántos antirretrovirales compramos. **(Aplausos).**

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

Por el Grupo Parlamentario Confederal de Unidos Podemos, tiene la palabra el señor Alonso.

El señor **ALONSO CANTORNÉ:** Gracias, señor presidente.

Saludamos la iniciativa del grupo del PDeCAT, que nos retorna a la realidad al plantearnos la necesidad de crear un método de trabajo viable y elaborar un informe de seguridad nacional dedicado a la política de la lucha contra el bioterrorismo.

La viruela ya actuó de forma devastadora contra la población mundial durante siglos —trescientos millones de muertos solo en el siglo XX— y hemos de evitar que se vuelva a repetir, evidentemente. Se cuenta que fuimos los españoles por medio de un esclavo africano los que introdujimos la viruela en América cuando la partida de Pánfilo de Narváez desembarcó en el Yucatán para intentar apresar a Hernán Cortés. Aunque las matanzas de Pánfilo de Narváez en Cuba, explicadas por fray Bartolomé de las Casas, pudieran hacernos dudar, el desembarco del que fuera adelantado de la Florida fue el primer acto de bioterrorismo de la humanidad documentado. Diezmó a la población azteca e inca, facilitando la conquista. Recordemos que el emperador Moctezuma falleció aquejado de la viruela.

Que sepamos, existen laboratorios que trabajan con el virus de la viruela como mínimo en Rusia y Estados Unidos, y esta es la pregunta que nos hacemos y se hacen algunos expertos: ¿Es necesario mantener el virus vivo? ¿Tenemos garantías de que un Gobierno como el de Estados Unidos, que en su día fue capaz de utilizar la bomba atómica contra la población civil dos veces, no pueda hoy, con el señor Trump al frente de la Casa Blanca, volver a cometer cualquier tipo de genocidio? ¿O de que el señor Putin utilice algún arma biológica con facilidad, cuando algunos Gobiernos occidentales le acusan de utilizar el polonio 210 contra personas? ¿Incluso otros países menos fiables que Rusia y Estados Unidos, por no hablar siempre de los grupos terroristas?

No tenemos respuestas ni certezas. Expertos nos hablan de que la viruela no supone una amenaza terrorista, y, en cambio, el ántrax, sí. Aunque sea por precaución, debemos seguir las recomendaciones de la OMS y no centrarnos exclusivamente en la viruela. Hemos de estudiar y valorar si, por ejemplo, las campañas antivacunas suponen un riesgo, como la aparición de nuevo del sarampión en España. Tampoco es descabellado trabajar para prevenir posibles actuaciones terroristas utilizando el chikungunya o el zika. Y para hablar de otro tipo de amenazas más cercanas, como vecino les pondré el ejemplo de la central nuclear de Vandellós II, que recientemente ha vuelto a vivir un incidente. Y aprovecho lo que publicó hoy el periódico *La Vanguardia* para sugerir si hemos de estudiar la acción del Gobierno belga,

cve: DSCG-12-CM-83

que desde ayer pone a disposición de la población que lo solicite y de forma gratuita pastillas de sodio en las farmacias, como parte de un plan de seguridad nacional.

La enmienda que presenta la señora Botella, por parte del Grupo Socialista, nos parece más completa, aunque también podríamos aceptar la del Grupo Popular. Pero no nos corresponde a nosotros, sino al PDeCAT, y estamos seguros de que dialogará y llegará a un acuerdo para que las enmiendas presentadas se puedan aceptar por todos los grupos.

Muchas gracias.

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

Quedamos a la espera de las negociaciones que hagan con los grupos.

Para la introducción histórica, le recomendaría también que leyese *Imperiofobia,* de Elvira Roca, que es un libro más ponderado que alguno de los que ha citado usted. Pero, en fin, esta es una opinión personal, abusando de mi posición de presidente de la Comisión.

Llegados a este punto, como ustedes saben, no tengo ningún inconveniente en que el grupo proponente y los grupos enmendantes tengan un turno más. Por tanto, la portavoz del Grupo Socialista tiene la palabra.

La señora **BOTELLA GÓMEZ:** Nos ratificamos en los términos establecidos en nuestra propuesta y, aunque la portavoz del Grupo Popular no nos ha incluido en esa posible transaccional, estamos dispuestos a que se logre algo que creo que es de tanto interés para este país como que esta iniciativa se apruebe por unanimidad.

Muchas gracias.

El señor **PRESIDENTE:** La representante del Grupo Popular tiene la palabra para explicarnos si están invitados al baile o no.

La señora **VÁZQUEZ BLANCO:** Señor presidente, cada uno busca la novia que quiere. En todo caso, no soy yo quien tiene que aceptar las enmiendas. Nosotros tenemos una sobre la mesa que seguimos defendiendo y hemos propuesto una transaccional.

Con respecto al portavoz de Podemos y lo malos que somos los españoles, que hemos infectado de viruela a medio planeta, lógicamente no voy a entrar en esas disidencias. Ya dije que no tengo la marca de la vacuna y él dijo que sí: en todo caso iría él a América a matar a gente, pero el Partido Popular no. En fin, estos son debates serios. Creo que tenemos amenazas reales. Me alegro de que nombrara también a Putin, no solo al señor Trump. En todo caso, vamos a hablar de Estrategia de Seguridad Nacional y bioterrorismo. Ciertamente, el otro día se publicaron algunas noticias preocupantes con respecto a la viruela y por eso está de actualidad. Pero no voy a ser yo y el Grupo Popular los que hoy escadalicemos o asustemos a la sociedad española, aunque esté de actualidad, después de lo sucedido recientemente.

Muchas gracias.

El señor **PRESIDENTE:** Gracias, señora Vázquez.

Lo que sí tengo que aclarar es que el portavoz de Podemos no estuvo en la expedición de Pánfilo de Narváez. Por tanto, no sé la responsabilidad que tendrá en este tema. **(Risas).**

— RELATIVA AL REFUERZO DE LAS CAPACIDADES DEDICADAS A LA LUCHA CONTRA LAS ACCIONES DE DESINFORMACIÓN. PRESENTADA POR EL GRUPO PARLAMENTARIO SOCIALISTA. (Número de expediente del Congreso de los Diputados 161/002652 y número de expediente del Senado 663/000050).

El señor **PRESIDENTE:** Pasamos a la siguiente proposición no de ley, relativa al refuerzo de las capacidades dedicadas a la lucha contra las acciones de desinformación, del que es autor el Grupo Parlamentario Socialista. Entiendo que la va a defender es señor Luena, quien tiene la palabra.

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

Después de este debate historiográfico y de alguna recomendación premiada hace poco bastante acertada, vamos con una iniciativa del Grupo Socialista que tiene un objetivo que es el de evaluar y reforzar los instrumentos de comunicación estratégica de España en el ciberespacio y en el seno de la

cve: DSCG-12-CM-83

Unión Europea, señorías. Con tres puntos: participar activamente en la construcción de estrategia en la Unión Europea que persigue detectar noticias falsas y las desinformaciones masivas y, por tanto, combatir su difusión; ampliar el rango de acción a las campañas de desinformación que se detectan respecto a los Estados miembros y reforzar de forma inmediata los medios humanos y materiales de un grupo que ya está creado el East StratCom Task Force perteneciente al servicio de acción exterior. Porque, señorías, la iniciativa del Grupo Parlamentario Socialista responde a una realidad: la proliferación en el espacio, en el ciberespacio, entendamos los medios digitales y las redes sociales, de noticias falsas, difamaciones personales, calumnias sobre instituciones u organismos, como decía antes desinformaciones masivas, todas ellas a través del ciberespacio.

Sin ir más lejos y por no hacer una glosa. El último año largo podríamos hablar de que situaciones como las descritas anteriormente se han dado en varios procesos políticos y electorales. Me he anotado aquí Holanda, Estados Unidos, las elecciones presidenciales, el referéndum del brexit en Reino Unido, Alemania, las elecciones legislativas, recientemente, el fin de semana pasado, Italia, y también en nuestro país Cataluña donde se ha detectado un aumento desproporcional de la actividad en medios digitales, redes sociales con un objetivo: influir en estos procesos a través de campañas de desinformación masiva y de injerencia. Más o menos he hecho una descripción objetiva de la realidad.

Señorías, esto no es nuevo en la historia. Lo nuevo es que el ciberespacio permite que el alcance de estas campañas y su propagación sea casi infinito. Estaremos de acuerdo, señorías, en que estas campañas que se basan en mentiras, en manipulaciones evidentes, comprobables, en desinformación masiva, si campan a sus anchas al fin debilitan los sistemas democráticos y los sistemas institucionales. Si campan a sus anchas los debilita. Nosotros creemos que el Estado de derecho debe actuar y por eso me gustaría leerles qué es lo que consideramos que debería hacer el Estado de derecho y sería garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques o a otro tipo de amenazas. En el marco comunitario, la estrategia global para la política exterior y de seguridad común incluye ya la ciberseguridad para asistir a los Estados miembros, les hablo de 2016, también habla de la autoprotección contra las ciberamenazas. Recientemente en noviembre de pasado año 2017 se ha creado un grupo de alto nivel. El Congreso y el Senado, las dos Cámaras de Estados Unidos están investigando sobre distintos autores, campañas y procedimientos. Francia, su presidente, ha anunciado ya también una ley contra las noticias falsas. Volviendo a la Unión, a nuestro marco de actuación lógico, ya existe ese equipo de 14 profesionales que trabajan en la detección de acciones de desinformación y que cuenta con una red «le llaman cazadores de desinformación» que tiene más de 400 expertos en 30 países.

Señorías, para terminar, lo que les pide el Grupo Parlamentario Socialista es el apoyo a esta iniciativa, porque creemos que ha llegado el momento de evaluar y reforzar estos instrumentos que acabo de mencionar rápidamente. Segundo, participar en la construcción de una estrategia europea contra la desinformación. Que seamos activos en esa estrategia, que ampliemos el rango de acción. Por último, algo que es consecuencia del anterior que reforcemos los medios humanos y materiales de los que disponemos hoy en día. El objetivo es combatir la desinformación masiva, combatir las noticias falsas, combatir las injerencias, porque, señorías, solo con definirlo no hacemos nada. Tenemos que actuar dentro del Estado de derecho y en el marco de una Unión Europea para que así no se debiliten nuestros sistemas democráticos. Muchas gracias por su atención, señor presidente. **(Aplausos).**

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

No hay enmiendas, solo puntualizar si le parece bien al señor Luena que en Estados Unidos no hay Congreso y Senado, sino Cámara de Representantes y Senado que forman juntos el Congreso, solamente matizar eso.

El señor **LUENA LÓPEZ:** Como aquí las Cortes Generales, perdón, señor presidente.

El señor **PRESIDENTE:** Perdónme usted por la impertinencia.

Ahora tiene la palabra el Grupo Mixto.

El señor **XUCLÁ I COSTA:** Muchas gracias, señor presidente, de esta Comisión Mixta de las Cortes Generales. Intervengo brevemente para anunciar el voto favorable a esta iniciativa que ha presentado el diputado don César Luena, apuntando que esta es una iniciativa de apoyo a una política de la Unión Europea, pero también debemos ir más allá de la Unión Europea para hacer una reflexión global, mundial

cve: DSCG-12-CM-83

sobre de qué forma Internet puede ser arbitrada sin que la neutralidad de Internet puede ser violentada, porque la libertad, el derecho al acceso a la información, que tenemos nosotros y que, por cierto, no tienen otros muchos países que viven con una libertad restringida a la información y al Internet. Este valor tan importante que es el acceso a la información tiene que venir compensado también por la veracidad de la información que circula por la red. Por esto se ha hablado del Ombudsman de Internet, se ha hablado de un árbitro de Internet, se ha hablado de la importancia de mantener un Internet neutro. Quiero destacar que esta es una iniciativa que apoya básicamente recomendaciones del Consejo Europeo de marzo del año 2015 respecto a países que son grandes productores y a veces víctimas de noticias falsas. La absorción oriental hace referencia a países concretos, a Moldavia que tiene elecciones este año y donde veremos los conflictos congelados cómo vuelven a ser muy vivos entre Moldavia occidental y Transnistria. Se hace referencia a Ucrania, donde la desinformación es también masiva. En cambio se ha hecho una referencia aprovechando que el río no pasaba por Madrid precisamente a la situación en Cataluña. Señor Luena, yo voy a apoyar su iniciativa porque tiene vocación de amplitud de miras, de apoyar una política de la alta representante de la Unión Europea y del servicio de acción exterior europeo, pero algún día será interesante que hablemos como ya se ha hablado en esta Comisión Mixta de la capacidad de la influencia sobre la información, sobre los *box*. Los *box* son estos artilugios para multiplicar los *retweets* y para multiplicar el número de seguidores, por ejemplo. Hay un dato relevante. *El Diario Independiente de la Mañana*, aquel que seguramente ustedes leían más cuando tenía una línea editorial más cercana, tiene más *box* para retweetear la información que produce que un medio al que nunca he decidido darle una entrevista o una información como *Rusia Today*. En Cataluña hay algunos retos muy importantes que no pasan precisamente por lo que usted de pasada ha dicho. Nuestro apoyo en todo caso a su iniciativa, que es una muy buena iniciativa.

El señor **PRESIDENTE:** Vamos ahora con el Grupo de Ciudadanos, señor Gutiérrez.

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

Intervengo muy brevemente para manifestarles que apoyaremos en este caso la proposición no de ley del Grupo Parlamentario Socialista, porque consideramos que está en línea y es de permanente actualidad. Hemos debatido e incluso dialogado en las comparecencias dentro de esta Comisión en estas semanas previas bastante sobre este tema. La desinformación ha sido una herramienta propia de los Estados para utilizarla desde tiempo inmemorial, no es algo nuevo. Digamos que ahora se ha actualizado porque los canales de acceso a la información se actualizan. Es cierto que tienen una virulencia mayor o la capacidad de hacer daño al final de un Estado sobre otro de determinados grupos de interés sobre incluso un propio Estado es potencialmente mayor que lo que eran los sistemas de desinformación históricos que siempre han existido en todos los conflictos entre Estados. Creemos —y coincidimos con ellos plenamente— que el Estado debe de protegerse frente a este tipo de amenazas. No voy a volver a destacar los casos en los que el señor Luena ya nos ha manifestado que ha habido pruebas demostrables de este tipo de ataques. Coincido en este caso con el señor Luena que en Cataluña también lo ha habido, aunque el señor Xuclà insiste que no. Nosotros creemos que es así y que debemos ver quién ha sido. Nos gustaría saber quién ha sido quien ha estado intentado desestabilizar al Estado español con esos ataques. Nada más lógico y sensato que apoyarse en los socios de referencia que siempre han sido. La Unión Europea, porque creemos firmemente desde Ciudadanos que es precisamente el espacio de convergencia donde probablemente tenemos que acabar haciendo cesiones incluso de soberanía para poder protegernos nosotros y llegar a políticas conjuntas dentro de ese gran Estado europeo que queremos crear entre todos los ciudadanos europeos. Nada más sensato que apoyarnos en aquellas infraestructuras que están creadas a las que debemos dar apoyo y de las que debemos servirnos. Los socios, esta es una batalla que no podemos hacer solos, necesitamos todos los socios posibles, y los tradicionales en otro tipo de estrategia son los que aquí debemos utilizar.

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

El señor Comorera tiene ahora la palabra.

El señor **COMORERA ESTARELLAS:** Gracias, presidente.

Ya les adelanto que mi grupo va a votar en contra de esta proposición no de ley. Ustedes reiteran el error que ya venimos observando en muchas ocasiones en esta Comisión que es mezclar la desinformación con la ciberseguridad o los ciberataques. Empieza la exposición de motivos de la PNL hablándonos del

cve: DSCG-12-CM-83

ciberespacio, de la ciberseguridad y de dar respuesta a los ciberataques para acabar afirmando que expertos y centros especializados han detectado un aumento desproporcionado en la actividad de redes sociales y medios digitales con el fin de influir en los procesos políticos y electorales. Los autores de tales campañas son desconocidos y las mismas no pueden ser calificadas de ciberataques, sino más propiamente procesos masivos de desinformación e injerencia. En qué quedamos son procesos de desinformación o ciberataques. Seguimos extendiendo la confusión general. La exposición de motivos de su PNL tiene una estrategia muy mala que es dividir entre malos y buenos. Discurso que ya hemos oído en esta Comisión. El potencial de desinformación a través de la red lo conocen los partidos políticos y Gobiernos de todo signo político. Hace años que los utilizan para sus propios intereses y aunque lo planteen como una novedad no lo es. Al final la intención que se desprende es la misma que pretende el Grupo Popular con sus iniciativas: un mayor control de la red a cambio de una supuesta mayor seguridad. Analizamos su PNL, dicen que la desinformación es un arma o herramienta casi tan antigua como la comunicación que la novedad reside en su difusión a través de medios digitales y redes sociales, lo que supone un salto cualitativo en su peligrosidad. Peligrosidad, porque no la controlan en su totalidad. Dan a entender que sería conveniente que el Est StratCom Task Force hubiese actuado en la supuesta campaña de desinformación en la crisis catalana. Por tanto están pidiendo que este organismo informe sobre una verdad. Yo les pregunto: ¿Habría pedido el PSOE que los cazadores de desinformación, como los denomina en la PNL, desacreditaran las informaciones o informes sobre las violentas cargas policiales del 1 de octubre? El proyecto periodístico *Maldito Bulo* se pasó el 1 de octubre desmintiendo informaciones que aparecían tanto del lado independentista catalán como del españolista, pero ustedes en su PNL solo se refieren a cuentas a favor del referéndum y de desinformación en relación con el proceso secesionista. ¿Están acaso ustedes desinformando en la propia PNL? La PNL hace referencia a reforzar las capacidades para luchar contra la desinformación. Este planteamiento no es concreto y genera confusión. El punto 3 de la PNL hace referencia al refuerzo inmediato en medios humanos y materiales del East StratCom Task Force. ¿Además de aumentar el personal, cuáles serían exactamente esos medios materiales? La dotación económica. Según algunas noticias el East StratCom Task Force tendrá por primera vez un presupuesto alrededor de 800 000 euros para 2018 con el objetivo de reforzar esta unidad en la lucha contra la supuesta desinformación. ¿Tenemos que facilitar más medios sin saber cómo se va a determinar qué es desinformar y qué no? Hace referencia a que se habría producido un incremento del 2000 % de la actividad de determinadas cuentas en redes y medios digitales a favor del referéndum. Lo mismo curiosamente que expuso Mira Milosevich en su intervención días antes en la Comisión Mixta de Seguridad Nacional, pero en ningún caso puede ser el argumento que se han producido ciberataques o desinformación. La propuesta de que España participe en el proceso de construcción de la estrategia de la Unión Europea para parar la difusión de noticias falsas en línea es un planteamiento peligroso. ¿Quién y cómo se determinan que noticias son falsas? Puede generar grandes recortes en derechos de los ciudadanos y por ahí no pasamos. A pesar de que la PNL insta al Gobierno a participar en la construcción de una estrategia en contra de la difusión de las noticias falsas, no expone qué son las noticias de desinformación, no las define o aporta datos que apoyen la demanda. El único dato no puede ser que se haya incrementado un 2000 % la actividad de determinadas cuentas en redes y medios digitales favorables al referéndum. Muchos expertos creen que si los Gobiernos quieren combatir la desinformación deben invertir en la alfabetización digital de la población y señalan que hay que generar una conciencia crítica para que los ciudadanos sean capaces de enfrentarse a estas informaciones. Hay que darles herramientas. Esa postura es la que defendía la propia vicepresidenta del Gobierno que añadía que el derecho a la información es uno de los más valiosos que existe y fundamental para la construcción de la libertad del individuo. Lo contrario es entrar en la censura y el control político de los medios de comunicación. La desinformación se combate con más información y no con censura. Además los primeros estudios independientes desmontan la alarma política sobre las noticias falsas y señalan que el análisis de la vida disponible sugiere que las noticias falsas tienen un alcance más limitado del que en ocasiones se asumen. Los regímenes totalitarios no son los únicos que utilizan la manipulación organizada de las redes sociales, explica un informe de la Universidad de Oxford. Ni siquiera son los mejores. Los primeros registros de Gobiernos revolviendo en la opinión pública son de democracias. Las nuevas innovaciones en las tecnologías de innovación suelen venir de partidos políticos y surgen durante campañas electorales de alto nivel. Estrategias como las que plantean y sin una palabra en toda la proposición no de ley sobre el respeto a derechos fundamentales como la libertad de expresión y la libertad de información nosotros no la vamos a apoyar. **(Aplausos).**

cve: DSCG-12-CM-83

El señor **PRESIDENTE:** Muchísimas gracias.
Por el Grupo Socialista, el señor Luena.

El señor **LUENA LÓPEZ:** Gracias por este turno generosidad de la casa, señor presidente.
Quiero agradecer las palabras del portavoz de Ciudadanos sobre la iniciativa además del apoyo que anunciaba. No está el señor Xuclà, por si acaso entra, voy a referirme primero a alguna palabra sobre la intervención del último grupo que acaba de hablar. Al escucharle atenta y respetuosamente su intervención he dicho qué justificada está la iniciativa del Grupo Socialista con esta intervención que acaba de hacer. No voy a entrar en un debate maniqueo, que creo que es donde se nos quiere llevar por parte del portavoz que acaba de intervenir. No voy a entrar. Fíjese hablaba usted de que hacía falta información y no censura, eso defiende esta iniciativa, pero hablamos de información veraz y contrastada. Para terminar, señor presidente, al señor Xuclà le agradezco mucho que haya anunciado que lo va a apoyar. Él sabe que la multiplicación de la desinformación o de noticias falsas en Cataluña, según algunos medios en el proceso del referéndum se multiplicó un 2000 %, según algunas informaciones, por eso era justificada que hiciese una breve intervención. Sé que se lo contarán o lo leerá en el «Diario de Sesiones», en todo caso que quede tranquilo el señor Xuclà porque los socialistas encajamos muy bien y nosotros leemos todos los periódicos escriban lo que escriban incluido un gran periódico como es *El Diario Independiente de la Mañana*, que supongo que se refería al periódico *El País*. Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señor Luena.
Cierra el debate de esta proposición, el señor Ramírez por el Grupo Popular.

El señor **RAMÍREZ RODRÍGUEZ:** Gracias, señor presidente.
Con la venia, la estrategia global sobre política exterior y de seguridad de 28 y 29 de julio del año 2016 señala que la Unión Europea centrará más su atención en la ciberseguridad dotando y ayudando a los Estados miembros de instrumentos para que se protejan mejor de las ciberamenazas y señalando que se aumentarán los esfuerzos en materia de defensa, cibernética, luchas contra el terrorismo y comunicaciones estratégicas. Por otro lado, la Estrategia de Seguridad Nacional del año 2017 recoge expresamente que una de las nuevas amenazas y desafíos a la seguridad nacional son los ciberataques combinados con acciones de influencia y desinformación lo que tiene además pensamos su corolario en la propia Estrategia de Ciberseguridad Nacional. La digitalización de la información y la entrada de las redes sociales como canal directo de comunicación con la audiencia, ha modificado tanto la producción como el acceso a la información. Pensamos desde el Grupo Parlamentario Popular que vivimos una nueva era la de la desinformación también en la que la pelea radica en hacer pasar el mensaje prescindiendo del rigor o incluso la veracidad del mismo, asistimos a fenómenos desconocidos hasta ahora. La utilización de fotos y videos antiguos atribuidos a hechos actuales, la agitación de sentimientos dirigidos contra objetivos prefijados o la financiación de nuevas técnicas de desestabilización. Las *fake news,* la guerra híbrida, como la denominan en los países bálticos, han llegado para quedarse. No cabe darles la espalda confiando en que la sociedad se muestre impermeable a una lluvia fina pero continua. El mismo hecho de salir en público a negar a desmentir una noticia que se ve que es falsa implica de alguna manera la difusión de la misma lo que ya puede ser aprovechado por algunos para dar carta a la difusión de ciertas mentiras a través de este propio desmentido. A nadie le debería sorprender que en breve quien protagonice el desmentido sea quien ha generado de un modo anónimo la noticia. Ante todo deberíamos plantearnos qué hacer. El señor Luena hablaba antes de la República Francesa y el presidente Macron que anunció su intención de prohibir las *fake news* durante sus campañas electorales para evitar estas injerencias. Sin embargo, nosotros pensamos que una prohibición es a todas luces imposible cuando se ha demostrado que su difusión no se realiza solo a través de un solo canal, sino que es múltiple, incluso a veces la difusión se realiza a través de la difusión de un solo canal que va a estar dedicado precisamente a esa múltiple producción de noticias falsas. La solución pensamos que no ha de venir de la desconfianza, sino de la confianza. La promoción de los medios acreditados. Buscar medios para ayudarles a recuperar su prestigio en la sociedad. Un prestigio que de alguna manera algunos tratan de poner en duda. No es un problema que afecte solo a España, como ya hemos visto y ya sabemos, sino que habría que buscar interlocutores con presencia en varios países. En prensa, como primera idea, puede ser alguna asociación que agrupe a un conjunto de medios internacionales como pudiera ser, por ejemplo, Lena, que es la unión de diarios europeos que fomenta la calidad. Que nos parece una buena iniciativa, un buen primer momento, pero también otros grupos mediáticos, empresariales, con presencia internacional.

cve: DSCG-12-CM-83

En nuestro grupo creemos que es la sociedad civil la que tiene que acreditar el trabajo. No basta con los premios de reconocimiento por la labor realizada, sino que es la hora de plantearse ofrecer al lector, oyente, espectador, herramientas que le permitan discernir la fiabilidad del medio a través del cual se informa. Algunos avances a nuestro entender han comenzado a producirse. Extensiones para navegadores como *Chrome* elaboradas por *webs,* como *Maldito Bulo,* al que hacía referencia el portavoz de Podemos, que permiten decir que estás navegando por una *web* que publica noticias falsas o informaciones difundidas en la red con los pasos a seguir para localizar el origen de una fotografía publicada. Sin embargo, todas ellas requieren de un esfuerzo por parte del lector oyente, espectador, y necesitamos saltarnos esos pasos previos, *banners* de colores dependiendo de la fiabilidad del sitio por el que navegamos, sellos o certificados que prueben la honorabilidad del medio o garantías que permitan verificar que el sitio no es una máquina de propaganda. El origen de las *fake news* sigue siendo muy discutible. Pero su difusión se hace a través de unas redes sociales públicas. No podemos permitir que una vez que hayan visto la luz se extienda ante la pasividad de una Administración cuya reacción muchas veces es tardía o pasa sin pena ni gloria alcanzando solo a una mínima parte de todos aquellos que ya han asumido la noticia falsa como propia. Hay un artículo muy interesante que se publica en *Bloomberg* lógicamente no voy a ha hacer demasiada mención, pero sí diré que en él se cita la labor llevada a cabo por los medios públicos como *Sputnik*. La elaboración de noticias perfectamente redactadas con fuentes constatables, pero donde la tergiversación llega de la selección de esas mismas fuentes. Uno realismo con criterios objetivos integrado por distintos representantes de la sociedad y con información oficial e inmediata no debería tener problemas a la hora de atajar una gran parte de esos bulos.

En suma, señorías, desde el Grupo Parlamentario Popular saludamos la iniciativa del Grupo Parlamentario Socialista, expuesta por el diputado señor Luena, y votaremos a favor de esta iniciativa por considerarla positiva y beneficiosa para generar una mayor concienciación y reconocimiento de esta realidad y pasar a ocuparnos cuanto antes del asunto de referencia. Muchas gracias. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, a usted, señor Ramírez.
Cerramos el debate de esta proposición.

— SOBRE LA ELABORACIÓN DE UN PLAN DE ACTUACIÓN INTEGRAL PARA EL FOMENTO DEL EMPLEO EN MATERIA DE CIBERSEGURIDAD. PRESENTADA POR EL GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO. (Número de expediente del Congreso de los Diputados 161/002899 y número de expediente del Senado 663/000060).

El señor **PRESIDENTE:** Pasamos a la siguiente proposición no de ley sobre la elaboración de un Plan de actuación integral para el fomento del empleo en materia de ciberseguridad de la que es autor el Grupo Parlamentario Popular, en cuya representación entiendo que va a hablar la señora Bonilla, tiene la palabra.

La señora **BONILLA DOMÍNGUEZ:** Muchísimas gracias, señor presidente.

Muy buenas tardes, señorías. La revolución de las tecnologías de la información y de la comunicación se ha convertido en la piedra angular del desarrollo económico. No estamos hablando de un sector económico específico, sino que estamos hablando del fundamento de los sistemas económicos innovadores modernos como viene contemplando de manera muy concreta la estrategia de mercado único digital en Europa. El espectacular crecimiento de Internet y de los servicios telemáticos, administración telemática, correos electrónicos, comercio electrónico, etcétera ha contribuido a extender mucho más el uso de la informática y de las redes de ordenadores hasta el extremo que en la actualidad no se circunscriben solo al ámbito laboral y profesional, sino que se ha convertido en un elemento que forma parte de lo cotidiano en la inmensa mayoría de los hogares españoles. Por otra parte, los sistemas y redes informáticas son el soporte de servicios críticos de nuestra sociedad moderna como son los servicios financieros, la propia Administración pública, instituciones, etcétera. Siendo eso así, además las nuevas tecnologías no solo son una piedra angular que ofrece múltiples e importantísimas oportunidades, sino que también suponen nuevos riesgos y amenazas a las que se enfrenta nuestra sociedad, nuestro país y el mundo en general.

Por todo ello, en la actualidad las actividades cotidianas, las empresas y las distintas administraciones públicas, así como de muchas instituciones y organismos requieren del correcto funcionamiento de los sistemas y redes informáticos que las soportan y sobre todo requieren de seguridad. Por ello la seguridad informática es esencial tanto en la actividad particular como pública y en la actividad profesional como en

cve: DSCG-12-CM-83

la personal. La amenaza de la proliferación de virus y códigos malignos y su rápida distribución a través de las redes como Internet, así como la de cientos de miles de ataques e incidentes de seguridad que se producen o pueden producirse todos los años nos demandan recursos y personal preparados para ello. Esto requiere formación específica de trabajadores, requiere personal preparado en empresas, administraciones e instituciones. Por tanto, es necesario orientar de una manera clara y decidida la profesionalización de los aspectos relativos a la ciberseguridad y a la ciberdefensa. Los planes formativos en TIC se desactualizan de manera muy rápida y especialmente los aspectos de seguridad requieren una permanente formación que permita la capacitación necesaria. Los principales países de nuestro entorno ya están llevando a cabo actuaciones innovadoras para la concienciación y formación de su personal y la generación de talento en ciberseguridad.

Por todo ello, desde el Grupo Parlamentario Popular proponemos este Plan integral para el fomento del empleo en materia de ciberseguridad. Con ello cubriríamos por un lado la parte de formación de aquellos trabajadores que ya se encuentran en trabajos vinculados a áreas de ciberseguridad y por otro ofreceríamos a muchas otras personas conocimientos y habilidades necesarias para acceder a un empleo o un tipo de empleo que tiene mucha demanda en la actualidad y, sobre todo la tendrá de manera creciente en los próximos años. Ya en el año 2014 el dictamen del Comité Económico y Social Europeo sobre ciberataques en la Unión Europea recogía la afirmación de que se prevé que la demanda de trabajadores de nivel universitario en el ámbito de la seguridad de la información como mínimo duplicaría la tasa de crecimiento global de la industria informática. En el informe de 2016 en *Infojob* se constata la existencia de unas 24 000 ofertas de empleo en este ámbito que no existían hace ocho años y en la misma línea la Comisión Europea estima que la demanda de empleos con cualificaciones digitales crece en torno a un 4 % anual y que el déficit de profesionales especialistas en el sector tecnológico de aquí al año 2020 podría alcanzar los 825 000 empleos vacantes dentro de la Unión Europea. Esta previsión es fácil que se incremente, debido a que la importancia creciente de las tecnologías de la información y la comunicación llevará a una mayor necesidad de estos profesionales.

Por ello, como decía antes, desde el Grupo Parlamentario Popular, instamos al Gobierno a elaborar un Plan de actuación integral para el fomento del empleo en materia de ciberseguridad que incluya entre sus líneas de actuación básicamente las siguientes: en primer lugar, actualizar los contenidos existentes del certificado de profesionalidad de seguridad informática para su adaptación a las necesidades del mercado laboral; en segundo lugar, la formación continua de trabajadores en las diferentes líneas de ciberseguridad, de impacto a corto y medio plazo; en tercer lugar, la creación de cursos de formación específica de ciberseguridad, a través del Servicio Público de Empleo Estatal, enfocados a la demanda existente en el mercado, con el fin de adecuar la oferta de trabajadores formados y formadores a lo que están demandando las empresas; en cuarto lugar, la oferta de diferentes cursos de formación profesional, específicamente en materia de ciberseguridad, que complemente la existente y que permita la oferta de un elevado número de trabajadores formados en ciberseguridad, a medio plazo; en quinto lugar, el fomento de la contratación de profesionales de ciberseguridad en las empresas y de formación de trabajadores ya existentes en plantilla, readaptando sus funciones; en sexto lugar, incluir en las medidas anteriormente propuestas a personal de los ministerios de la Presidencia, Defensa, Interior e Industria, Energía y Turismo; y en séptimo lugar, fomentar la colaboración en sus respectivos ámbitos de competencia con las comunidades autónomas, así como la consulta con los agentes sociales.

Señorías, como decía al principio de mi intervención, las redes sociales son una enorme oportunidad no solo para la participación sino para la interconexión entre las empresas y el crecimiento de estas. Los delincuentes siempre han estado alerta sobre nuevos medios que puedan ser utilizados para facilitar actividades delictivas. Los efectos multidisciplinares de los riesgos y amenazas en el ámbito del ciberespacio obligan a una preparación en todo el espectro de competencias de las administraciones públicas. Los organismos con principales responsabilidades en tratar de combatir estos riesgos y amenazas están adscritos a los ministerios de Presidencia, Defensa, Interior e Industria, Energía y Turismo. Por tanto, señorías, debemos contar con todo el talento preparado y permanentemente capacitado para la inserción laboral, pero también para el reciclaje, la continuidad y el desarrollo profesional.

Respecto a las enmiendas presentadas por dos grupos quiero decir que sí vamos a admitir la enmienda del Grupo Ciudadanos, como ya le he comentado a su portavoz. Además, está muy línea con el espíritu de nuestra proposición en el sentido de que la enmienda del Grupo Ciudadanos dice textualmente: «Reforzar la colaboración público privada en el ámbito de la ciberseguridad para alcanzar

cve: DSCG-12-CM-83

mayores resultados tanto en el ámbito tecnológico como empresarial, con el fin de afrontar mejor las amenazas de ciberataques, así como de reforzar la competitividad de las empresas del sector.

Para finalizar, señorías, pido el apoyo de todos los grupos a esta iniciativa porque creo que es muy importante para España. Hemos de tener y preparar a un número de personas suficientes para que se puedan cubrir nuevas plazas tanto públicas como privadas para atender a la creciente demanda de la seguridad de las TIC y la inversión en formación, a fin de dotar a España del personal experto para hacer frente a las ciberamenazas con carácter preventivo tanto en empresas como en centros de gestión de incidentes y protección de infraestructuras críticas, y en organismos de la Administración pública.

Muchísimas gracias. **(Una señora diputada: ¡Muy bien!).**

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

Para la defensa de sus enmiendas tiene la palabra, por el Grupo Parlamentario Ciudadanos, el señor Salvador.

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

En primer lugar, independientemente de que vayamos a votar a favor del conjunto de medidas deslavazadas que se plantean y que se tratan de vender como un Plan de actuación integral en el fomento del empleo, desde mi grupo queremos matizar varias cuestiones. Todos estamos de acuerdo con la importancia de la ciberseguridad. Por eso tenemos una ponencia en esta Comisión, precisamente para que comparezcan expertos y para que a partir de todas esas aportaciones tengamos de verdad un Plan integral contra la ciberdelincuencia en nuestro país, que englobaría muchas cosas, entre ellas, también la necesidad de cubrir la carencia de profesionales que pudiera haber.

En una intervención anterior, un compareciente nos cifraba la semana pasada el coste de inseguridad en 2015, que ascendía a los 700 billones de dólares —hablaba de trillones americanos— para el año 2030. Se mencionó que la amenaza antiterrorista estaba en el nivel 4, las infraestructuras críticas en el nivel 4, las ciberamenazas estaban en un nivel de alerta muy alto, así como que la estrategia de nuestra industria 4.0 y de la transformación digital necesitaba cubrirse con profesionales pero que en este momento no teníamos esa capacidad. Daba un dato muy interesante cuando decía que el 82 % de los consejos de administración tenían ya incluidos en su agenda la ciberseguridad y, por tanto, se supone que podían preparar planes para acometer esa inseguridad. Al mismo tiempo el compareciente preguntaba: ¿Y las pymes? Las pymes en este momento en España están absolutamente sueltas. Nosotros vemos que estamos poniendo el carro por delante de los bueyes. Es decir, queremos lanzar un plan de desarrollo de profesionales cuando no sabemos ni siquiera cuál es el plan que tenemos que acometer, para a partir de ahí tener la especialización necesaria para poder llevarlo adelante, entre otras cuestiones.

Les pongo un par de datos como ejemplos. Si nosotros necesitamos, por una parte, hacer reformas en la educación, y por otra parte, también en la cultura del mundo de las pymes y la Administración, no entendemos por qué no se acepta nuestra enmienda que propone la creación de un CISO, director de seguridad de la información, responsable de implantación de los sistemas de seguridad de información en la Administración General del Estado, cuando no tenemos un estándar de ciberseguridad en cada uno de los ministerios que sea común para todos. Por tanto, en la Administración General del Estado no tenemos homologada ni estandarizada cuál es la respuesta que vamos a dar a la ciberseguridad, pero aquí estamos sugiriendo que se contraten deslavazadamente a profesionales sin ningún tipo de plan para saber exactamente en qué tienen que instruirse.

Voy a dar otro dato. En las ingenierías informáticas no se incorpora la asignatura de ciberseguridad como tal para tener profesionales de seguridad. Ese es uno de los cambios que entendemos que habría que hacer, porque ya que estás fabricando ingenieros informáticos, si además una parte de ellos tienen una especialización importante en ciberseguridad, ahí estás sacando profesionales preparados. Por ejemplo, en Estados Unidos en 2015 no se cubrieron 250 000 plazas necesarias de ciberseguridad, porque no tenían la formación adecuada para ello. No creemos que eso se solucione diseñando unos pocos cursos por aquí o metiendo algunas asignaturas en formación profesional por allá, ni fomentando que se contrate en las empresas cuando no tenemos un plan que ofrecerles todavía.

Esta proposición no de ley tiene buena intención y nosotros la vamos a apoyar. Nos han dicho que aceptan nuestra enmienda que habla de la colaboración público privada, pero también habíamos presentado otras que embridaban la Administración General del Estado y planteaban tener un plan y una persona responsable. Asimismo, nosotros no estamos para fomentar la contratación de las empresas de este personal, otra cosa es favorecer que surjan los profesionales necesarios y que las empresas

cve: DSCG-12-CM-83

conocedoras de la inseguridad sean las que decidan cómo pueden paliarla y si quieren profesionales o no. Por tanto, nosotros vamos a apoyar la iniciativa que han presentando, pero, eso sí, el Plan de actuación integral para el fomento del empleo no lo vamos a tener porque aprobemos hoy estas medidas. Tendremos unas poquitas medidas, pero en la ponencia que hagamos al final sobre ciberseguridad tendremos que recoger ese plan con unas medidas mucho más contundentes que den respuesta al diagnóstico que hayamos establecido también cuando se cierre esa ponencia.

Muchas gracias.

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

Por el Grupo Parlamentario de Unidos Podemos, tiene la palabra la senadora Angustia.

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

Nosotros entendemos que las propuestas que nos hace hoy el Partido Popular evidentemente tienen la voluntad de resolver un déficit de formación en materia de ciberseguridad, tanto en el ámbito público como en el ámbito privado, pero echamos en falta dos cosas. Primero, no entendemos el porqué los grados no aparecen incluidos en las posibilidades de formación, es decir, por qué no se incluye la formación a todos los niveles medios y superiores de forma transversal en educación reglada, ya sea en ciclos, grados o formación profesional, susceptibles de tratar el tema de ciberseguridad. Y segundo, echamos de menos, sobre todo, el marco global que debería de poner los cimientos para este tejado, que al fin y al cabo es la moción. Han empezado la casa por el tejado, pero nosotros pensamos que habría que empezar por el principio real que sería, si estamos hablando de formación, por alcanzar un pacto educativo, es decir, un plan estratégico que a largo plazo nos permita no solo resolver las deficiencias en materia de seguridad a nivel profesional, administrativo, y a nivel de seguridad de los propios ciudadanos y ciudadanos, sino además tener una estrategia a largo plazo y no una pura solución táctica que evidentemente —permítanme que lo diga— es totalmente susceptible de manipulación política por parte del Gobierno que pretenda llevarla acabo.

El informe del Foro Económico Mundial titulado «El futuro de los trabajos 2016: Empleo, habilidades y estrategia de la fuerza de trabajo para la cuarta revolución industrial» afirma que las profesiones y competencias más demandadas en la actualidad no solo no existían hace diez o incluso cinco años, sino que el 65 % de los niños que ahora estudian primaria trabajarán en empleos que todavía no existen. Por lo tanto, entendemos que abordar la formación en ciberseguridad es una cuestión estratégica, una cuestión de futuro, y no una cuestión meramente táctica que nos permita resolver deficiencias solo a corto plazo.

Por todo ello presentamos esta enmienda, porque creemos que es imprescindible convocar a agentes públicos y privados implicados. Nuestra apuesta para ese desarrollo de futuro, para ese desarrollo estratégico, sería precisamente sentar las bases con distintos organismos —cito, aunque seguramente se me escapen algunos—, con el Gobierno, con los grupos parlamentarios representados en el Congreso y en el Senado, con los partidos políticos, con el Consejo Nacional de Seguridad como responsable de la ciberseguridad dentro del Consejo Nacional de Seguridad Nacional, con el Instituto Nacional de Ciberseguridad, con el CERT, con el Mando Conjunto de Ciberdefensa, con el Centro Tecnológico, con el Incibe, etcétera, es decir, con todos los agentes privados y públicos para que se sienten a esa mesa —permítanme que vuelva a llamarlo pacto educativo—, si de verdad lo que queremos es una estrategia de futuro que contemple la formación en ciberseguridad. Una vez alcanzado este pacto, una vez sentadas las bases, una vez que sepamos lo que queremos hacer lo dotaremos económica y técnicamente, lo dotaremos de recursos humanos. A partir de ahí podemos implementar todas las medidas que propone el Partido Popular en su proposición no de ley, así como otras muchas que puedan salir derivadas de esos criterios del Pacto estratégico para la formación en ciberseguridad.

Muchas gracias. **(Aplausos).**

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

A continuación pasamos al turno de fijación de posiciones. Ruego a los intervinientes que se ciñan a los tres minutos. En primer lugar, por el Grupo Parlamentario Mixto, señor Xuclà.

El señor **XUCLÀ I COSTA:** Muchas gracias, señor presidente. Mi intervención será más breve todavía.

Quiero expresar el voto favorable del Partit Demòcrata a esta iniciativa del Grupo Popular. Qué duda cabe que la creación de nuevos puestos de trabajo vinculados con la ciberseguridad es una realidad.

cve: DSCG-12-CM-83

Como apuntaba el Comité Económico y Social Europeo en su informe del año 2014, en diez años se van a multiplicar por dos los trabajos de nivel universitario vinculados al ámbito informático de la ciberseguridad. Finalmente, y no es juego, siempre será mejor la formación reglada que la formación no reglada. El último gran ataque mundial de ciberseguridad fue resuelto por unos jóvenes *hackers* que detectaron primero la solución, antes que los grandes sistemas de inteligencia y de lucha contra el ciberterrorismo. Por tanto, es bueno que se incorpore en el sistema aquellos que más saben y es bueno que aquellos que más saben estén dentro de los centros de lucha contra el ciberterrorismo.

Muchas gracias.

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

De acuerdo con lo que hemos establecido en la proposición anterior, tiene la palabra para mostrar su posición sobre las distintas enmiendas, por el Grupo Parlamentario Ciudadanos, el señor Salvador.

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

He manifestado antes que son medidas que no vienen mal y que se pueden llevar adelante. Aunque no entendamos que sea un plan, vamos a apoyar la proposición no de ley.

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

Por el Grupo Parlamentario de Unidos Podemos, senadora Angustia.

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

Parece que en lo que sí estamos de acuerdo todos y todas es que las tecnologías de la información han sido incorporadas absolutamente a todos los ámbitos de nuestra vida. Compramos, vendemos, hacemos transacciones telefónicas, nos relacionamos con la Administración pública, hacemos gestiones relacionadas con sanidad, con educación, con gestión de transportes, etcétera, a través de las nuevas tecnologías. Por tanto, la seguridad también tiene una increíble dependencia desde que se produce este cambio de las nuevas tecnologías. Si la seguridad interna y la seguridad externa empiezan a tener líneas muy difusas, más difusas son todavía las líneas en el marco de la ciberseguridad. La ciberseguridad no deja de ser un espacio transversal y un espacio global. Por tanto, tratar este espacio exige también en materia de formación la implicación y la coordinación de absolutamente todos los actores públicos y privados, de todas las autoridades competentes, de las Fuerzas y Cuerpos de Seguridad, de la industria, del mundo académico y de la ciudadanía, exactamente igual que cuando hablamos de formación.

El Centro Mundial de Seguridad Cibernética y Educación después de recoger a través de veinte mil asociaciones datos en ciento setenta países ha concluido que en 2022 tendremos una escasez de casi dos millones de trabajadores y de trabajadoras en materia de seguridad. Aquí quiero incidir cuando digo trabajadoras. Tenemos la oportunidad de no crear una nueva brecha de género, porque además de lo que nos alerta el Foro Económico y Mundial es de que existe una brecha de género en este campo. Sin embargo, ninguna de las medidas que se nos proponen en la moción van encaminadas a no generar una nueva brecha de género, que sufrimos las mujeres en la creación de empleo, en materia de ciberseguridad. Creo que es necesario reflexionar sobre este asunto.

Tanto la Estrategia de Seguridad Nacional de 2013, como la Estrategia de Seguridad Nacional de 2017, identificaban doce riesgos y amenazas para la seguridad nacional, y entre ellas, identificaba riesgos y amenazas en la ciberseguridad. Para alcanzar los objetivos de fortalecer nuestras capacidades de prevención, de detección y de respuesta a los ciberataques, así como para garantizar el uso seguro de las redes y de todos los sistemas de información, se proponían seis líneas de acción. De estas seis líneas de acción, cinco de ellas están relacionadas con medidas formativas. Esto ocurría en la estrategia de 2013 y esto vuelve a ocurrir en la estrategia de 2017. ¿Qué es lo que hacen las estrategias? Determinar necesidades. Pero estaremos de acuerdo en que los grados de profesionalización, de especialización y de perspectiva, son totalmente diferentes a la hora de abordar las soluciones, que a la hora de hacer la detección de necesidades.

Voy terminando, presidente. Por eso proponemos esa mesa de agentes públicos y privados y de expertos, porque si no el Gobierno puede —permítanme que incida en eso— desarrollar una propia campaña de desinformación. Hago un último apunte. Si lo que pretendemos es tener una estrategia formativa de futuro, vuelve a ser necesaria la cooperación multidisciplinar también en los ámbitos europeo e internacional. Tampoco nos dicen cómo van a abordar esas medidas en su moción. Esto lo hacemos porque nosotros apostamos por las decisiones tomadas en los espacios más amplios posibles, rigurosos,

cve: DSCG-12-CM-83

participativos y profesionales. Y esto lo hacemos porque no apostamos por los recortes de derechos en la red, ni apostamos por una reducción de la privacidad en las redes para los ciudadanos y las ciudadanas.

Muchas gracias.

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

A continuación, por el Grupo Socialista, tiene la palabra la señora Nasarre.

La señora **NASARRE OLIVA:** Muchas gracias, presidente.

Con respecto a esta proposición acerca de la elaboración de una Plan integral para el fomento del empleo en materia de ciberseguridad desde el Grupo Socialista en cierta manera coincidimos con el fondo, pero no con la forma; coincidimos con el fondo concepto, pero no con la forma ejecución. No queremos seguir en el estudiar, en elaborar un plan, en fomentar, sino que ya debemos establecer unos plazos y criterios, una ejecución presupuestaria y apuesta claros.

Señorías, estamos inmersos en un periodo de transformación digital que va mucho más allá del empleo en el sector de la ciberseguridad, que va mucho más allá del fomento del empleo, va de calidad en ese empleo, va de generación de un empleo adecuado, con más medidas y formación particular y con unas necesidades diferentes, con horarios distintos, con características especiales que como políticos y representantes públicos debemos afrontar con compromiso y responsabilidad. El entorno digital hoy se encuentra en un modelo de transición en el mundo laboral digital, que ya no solo abarca al sector de la ciberseguridad sino que va más allá. Debemos tener claro que la colaboración público privada y su coordinación es esencial. No actúen con políticas caducas que rebozan con su reforma laboral de la precarización y la poca innovación enmarcada en la temporalidad inestable, sino que deben apostar por estar actualizándose en los distintos sectores, adecuándose a las necesidades; innovando y apostando por la formación profesional; colaborando con las universidades; anticipándose a la demanda para fortalecer un sector importante del que depende el futuro de nuestro conocimiento digital como país y que puede desarrollar e impulsar una mejor sociedad productiva y adaptada al momento complicado y difícil en el que estamos para afrontarlo con garantías y con la máxima seguridad.

Por lo tanto, coincidimos en el diagnóstico, pero no en las pautas a seguir para paliar el déficit del desarrollo en el sector. Creemos que hace falta un impulso decidido y no afrontarlo desde la demagogia. No puede el Gobierno, la vicepresidenta, anunciar la creación de un Centro de operaciones de ciberseguridad y luego tener en Defensa un Mando Conjunto de Ciberdefensa. Queremos creer que es descoordinación y no guerras internas, o quizá sea una desinformación en el propio Partido Popular. En todo caso, ni una cosa ni otra nos parecen razonables. Deben centrarse en la coordinación de los distintos ministerios, de las comunidades autónomas y las entidades locales, así como con las empresas, de un modo transversal. Apoyaremos la proposición, pero estaremos atentos como oposición responsable y preocupada por el momento actual en el que estamos, porque desde este Gobierno parece que le cuesta afrontar y tomar decisiones. Estaremos vigilantes, atentos y reivindicaremos mayor eficacia en la mejora en la ciberseguridad, en el fomento del empleo y del talento, en el conocimiento en el sector. Esta es la mejor forma de combatir las amenazas y generar seguridad; seguridad para adaptarnos y adecuarnos al futuro que, señorías, es ya presente.

El señor **PRESIDENTE:** Muchas gracias, senadora Nasarre.

Este turno lo cierra, por el Grupo Parlamentario Popular, la señora Bonilla.

La señora **BONILLA DOMÍNGUEZ:** Muchas gracias, presidente.

Después de escuchar a todos los portavoces, y dar las gracias de antemano a todos los que han anunciado que van a apoyar esta iniciativa, sinceramente hay algunas posiciones que no entiendo. Yo creo que estamos de acuerdo todos en la necesidad de que hay nuevas expectativas en el mundo de la digitalización que suponen nuevas oportunidades, pero que también suponen unos riesgos. Tenemos que tener en cuenta que estamos hablando de nuestra vida diaria, pero estamos hablando también de las empresas de desarrollo económico y estamos hablando de servicios críticos, como pueden ser la seguridad, etcétera. ¿Qué es lo que quiere el Grupo Popular? Se ha detectado —así están los datos y los hemos enunciado varios portavoces— que hay una necesidad imperiosa de personas que estén habilitadas y que tengan los conocimientos suficientes para garantizar un correcto funcionamiento, por un lado, para prevenir posibles ataques, y por otro, para estar capacitados para reaccionar ante esos posibles ataques.

cve: DSCG-12-CM-83

¿Qué proponemos? Nosotros proponemos toda una serie de medidas que hemos denominado un plan integral, porque entendemos que cubre los espacios que tenemos ahora mismo —además lo he dicho varias veces en mi intervención— a corto y a medio plazo. Eso no es incompatible con un plan estratégico a nivel nacional y con proyección larga; eso no quiere decir que en esta iniciativa nosotros pretendamos abarcar todo lo que supone la ciberserguridad en España y en el mundo. A mí me parece sinceramente que aquí tenemos que analizar si esto es bueno para nuestra sociedad, para nuestras empresas y para los trabajadores. Aquí hemos elegido un ámbito muy amplio, hemos cogido personas que no tienen trabajo y que podrían ser personas perfectamente capacitadas con los conocimientos suficientes para tener la oportunidad de tener este trabajo y cubrir, por un lado, la necesidad de ese puesto de trabajo, y por otro, tener la oportunidad de trabajar. Hemos cubierto a personas que ya están dentro del ámbito de este sector, pero que necesitan más conocimientos; hemos cubierto el ámbito de las administraciones y hemos hablado de ministerios tan importantes que afectan a nuestra seguridad, como Interior, Defensa, etcétera. Nosotros proponemos que en esos diversos ámbitos se hagan estas actuaciones por parte del Gobierno. Un Gobierno que está preocupado y ocupado, entre otras cosas, por el desarrollo económico y por las empresas que generan empleo y oportunidades, así como por la seguridad de los ciudadanos.

Por tanto, señorías, permítanme que les diga que, sin perjuicio de que queda mucho y es verdad que hay una ponencia donde se están aportando por los expertos opiniones y datos muy interesantes, creo que no pasa nada por reconocer que esta propuesta tiene contenido y que es buena para la sociedad española, que es lo que les estamos planteando.

Solo quiero hacer un apunte, y me voy a referir a las dos enmiendas. En cuanto a las enmiendas del Grupo Ciudadanos tengo que decirle a su portavoz, con todos los respetos, que no puede decir aquí que los ingenieros informáticos no hablan de ciberseguridad. Dígame usted qué es un virus y cómo los ingenieros informáticos precisamente están preparados para actuar. Que me diga que quiere un plan más ambicioso, vale, pero que diga que no tocan la ciberseguridad creo que como argumento no puede servir.

Respecto a la enmienda del Grupo de Unidos Podemos, quiero decirles que mezclan el tema de la universidad y de los grados, con la posibilidad de incluir los temas de ciberseguridad en la educación. Estamos ahora mismo en un Pacto por la educación —por cierto, también aprovecho para decir que ojalá el Grupo Socialista se vuelva a sentar, porque es muy importante—. Aquí estamos hablando de lo importante que es en la educación la materia en ciberseguridad y lo importante que es para todos los ciudadanos y para todos los niños esa educación. Precisamente, como estamos en un pacto, todo esto lo tendremos que tratar dentro de ese ámbito. En definitiva, y sin perjuicio de que haya muchas cosas que podemos hacer más, yo les invito a que presenten otras iniciativas porque están en su derecho. Sin embargo, creo que honestamente esta propuesta del Partido Popular ofrece oportunidades para el empleo, oportunidades para la seguridad, tanto a nivel de empresas como de administraciones públicas. Así que les agradezco sinceramente su apoyo a los que han dicho que sí, y a los que no se han pronunciado les agradecería su voto favorable. **(Aplausos.—Un señor diputado: ¡Muy bien!).**

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

— RELATIVA A LA «DESINFORMACIÓN» Y SU RELACIÓN CON LA CIBERSEGURIDAD EN ESPAÑA. PRESENTADA POR EL GRUPO PARLAMENTARIO CONFEDERAL DE UNIDOS PODEMOS-EN COMÚ PODEM-EN MAREA. (Número de expediente del Congreso de los Diputados 161/002908 y número de expediente del Senado 663/000061).

El señor **PRESIDENTE:** A continuación pasamos al punto 4.º, y último, del orden del día: proposición no de ley relativa a la desinformación y su relación con la ciberseguridad en España, presentada por el Grupo Parlamentario Confederal de Unidos Podemos. Para su defensa, tiene la palabra el señor Del Olmo.

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

Hoy presentamos una proposición no de ley sobre la desinformación, que me gustaría resaltar que no es igual a la que ha presentado el Grupo Socialista, aunque el título pudiera confundir. Para comprobarlo bastaría que escuchasen la intervención de hoy del señor Luena y luego la comparasen con cualquier otra de la señora De Cospedal, porque no habría ninguna diferencia. Su proposición no de ley es un pase de gol a la propuesta que presentará en Pleno el Partido Popular el próximo martes.

cve: DSCG-12-CM-83

Vayamos a lo importante. Señorías, las tecnologías de la información y la comunicación se han incorporado a todos los ámbitos de nuestras sociedades, favoreciendo un desarrollo incuestionable tanto en el sector público como en el sector privado. En Internet compramos y vendemos bienes y servicios, realizamos gestiones en banca electrónica, desarrollamos actividades clave para la estabilidad y la prosperidad económica de los Estados, como pueden ser la gestión de los transportes, la sanidad o la energía. Como no podía ser de otra forma, en el ámbito de la seguridad encontramos también una mayor dependencia de las tecnologías de la información y la comunicación, lo que a su vez supone la aparición de nuevas vulnerabilidades y nuevos desafíos, en relación con la protección de infraestructuras críticas, el crimen organizado o el terrorismo. Los retos actuales que presenta la ciberseguridad están modificando las concepciones clásicas de la seguridad en un mundo globalizado. Si actualmente la línea que separa la seguridad interior de la exterior es muy difusa, en el ciberespacio como ha dicho algunos de los comparecientes de esta Comisión es casi inexistente. Por lo anterior, y por la importancia de este asunto, no podemos compartir con la mayoría de partidos políticos aquí que se equiparen los conceptos de ciberguerra y desinformación, porque se está haciendo con intereses políticos y al hacerlo así se juega con la seguridad de los ciudadanos. No tiene otro motivo esta alarma que se está creando entre los ciudadanos.

La proposición no de ley que ha presentado mi grupo aquí insta al Gobierno a: Primero. Desarrollar políticas en materia de ciberseguridad que cumplan la legislación nacional e internacional sobre derechos fundamentales de la ciudadanía. Cualquier iniciativa que desarrolle el Gobierno deberá respetar lo establecido en el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 10 del Convenio Europeo de Derechos Humanos y el artículo 20 de la Constitución española. Segundo. Abstenerse de utilizar posibles incidentes que puedan afectar a la seguridad tanto del Estado como de la ciudadanía como pretexto para recortar derechos fundamentales. Todo tipo de planes de seguridad y buenas prácticas que el Gobierno pretenda implementar no deberán incluir medidas que obliguen a la identificación en Internet o la restricción de acceso a la red a los usuarios que han optado por el anonimato. Los poderes públicos ya disponen de mecanismos suficientes, dentro de su ámbito de actuación, para perseguir los delitos en Internet. Tercero. Evaluar y reforzar los recursos y mecanismos legales existentes para perseguir con mayor eficacia los posibles actos delictivos que se cometan utilizando las tecnologías de la información y la comunicación. Cuarto. Todas las propuestas y recursos deben establecerse sobre la base de la Unión Europea y en defensa de los intereses nacionales, y nunca de intereses privados. Por último, extender el conocimiento de la ciudadanía sobre cuestiones relativas a la ciberseguridad. En este sentido, el Gobierno debería ponerse de acuerdo, ya que son conocidas las diferencias que mantienen en este ámbito la señora Cospedal y la vicepresidenta Soraya Sáenz de Santamaría. El Gobierno debería abstenerse de implementar cualquier iniciativa o mecanismo administrativo que pretenda determinar la veracidad de las informaciones que circulan por Internet, así como establecer un sellado de noticias falsas. En resumen, señorías, una vez más es el Grupo de Unidos Podemos el que tiene que recordarles aquí que hay que cumplir la ley.

Para terminar, una última cuestión. El Grupo Parlamentario Ciudadanos ha presentado una enmienda para que eliminemos la parte en la que instamos al Gobierno a que no desarrolle medidas contra el anonimato en la red, algo que seguramente sería inconstitucional. En palabras de uno de los comparecientes en esta Comisión, el señor Sánchez Almeida, el ciudadano tiene derecho a ser anónimo y el Estado, a través del Poder Judicial, puede levantar ese anonimato en caso de delito. No vamos a poder aceptar esa enmienda que ha presentado Ciudadanos.

Muchas gracias.

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

Para explicar esa enmienda, y cualquier otra precisión que quiera hacer, tiene la palabra el señor Salvador.

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

En primer lugar, cuando hablamos del mundo digital estamos hablando de que es exactamente igual que el resto del mundo, independientemente de nuestras actuaciones dentro del marco digital, pero no debería ser diferente, en ningún sentido, de lo que sucede fuera de ese marco y de ese ámbito. También es verdad que, precisamente igual que la tecnología y la comunicación provocan avances que son evidentes para todo el mundo, esa tecnología mal utilizada provoca amenazas a las que hay que dar respuesta en este momento. El Grupo de Unidos Podemos permanentemente intenta romper un poco el

cve: DSCG-12-CM-83

concepto de desinformación; la desinformación como una herramienta que utilizan personas para influir en las opiniones públicas y para cambiar incluso el ejercicio de la democracia. Si a la ciudadanía la engañas con una información que cree veraz, que está manipulada, lo que permite una intención de voto distinta de la que tenían pensada si la información que tuvieran hubiera sido otra, estamos hablando de una amenaza que toca los pilares fundamentales de nuestra democracia y de un Estado de derecho.

Cuando el Grupo de Unidos Podemos habla de que hay que defender los derechos fundamentales, Ciudadanos está absolutamente de acuerdo, faltaría más, y hay que garantizarlos de acuerdo con toda la normativa internacional y con la de nuestro país. Pero cuando el Grupo de Unidos Podemos relaciona los conceptos libertad de expresión y anonimato y los junta para defenderlos, entendemos que o bien oculta algo o bien está equivocado. ¿Las operaciones financieras no tienen trazabilidad? ¿Eso no permite combatir el terrorismo, el blanqueo de capitales? En un momento determinado, las personas nos tenemos que identificar en un banco para que se sepa que las transacciones que estamos haciendo son nuestras. Esto está a la orden del día, porque hasta en el cajero te sale que presentes tu cuenta en tu banco. Todo depende.

Cuando se habla de libertad de expresión, por supuesto que estamos de acuerdo, ¿pero libertad de expresión es incitar a la violencia? ¿Libertad de expresión es insultar gratuitamente a personas? ¿El anonimato debe amparar eso? ¿No hay campañas organizadas contra personas, contra instituciones por personas que valiéndose del anonimato cobarde permanentemente están tratando de desfigurar actuaciones del día a día, repito, de personas o de instituciones? No se puede meter el anonimato dentro de Internet como una excusa para poder hacer lo que quieras, porque los derechos fundamentales de cada uno terminan donde empiezan los derechos fundamentales del vecino que tenemos al lado. Cuando yo ejerzo mi libertad de expresión en Internet tengo que tener cuidado de no vulnerar los derechos fundamentales que tienen otros ciudadanos de no ser agredidos, de no ser señalados por mí para que otras personas les puedan atacar poniendo sobre ellas el foco, como se hace actualmente.

No hemos dicho que en la enmienda quitábamos el punto de los derechos fundamentales, la libertad de expresión y el anonimato en Internet. Voy a leer el principio de ese punto, en el que instan a la criminalización de los Gobiernos basándose en teorías de la conspiración, que dice: Abstenerse de utilizar posibles incidentes que puedan afectar a la seguridad tanto del Estado como de los propios ciudadanos, como pretexto para recortar derechos fundamentales. Se refiere al Gobierno. ¡Cómo que abstenerse! ¿Presuponemos que un Gobierno utiliza esa excusa de tratar de solucionar un problema premeditadamente para aprovechar y hacer un recorte de los derechos fundamentales de los ciudadanos? ¿Entendemos que esa libertad de expresión no conlleva también la política de difamación o distorsión de la realidad? ¿Negamos que las campañas de desinformación en este momento son un problema que se está analizando y estudiando a nivel mundial, con datos empíricos de dónde se producen los ataques, qué tipo de información introducen y qué tipo de realidad tratan de cambiar para convertirla en una posverdad?

Estamos de acuerdo con la parte propositiva del Grupo de Unidos Podemos, en el sentido de querer defender los derechos fundamentales del conjunto de los ciudadanos, seguir la normativa europea y respetar la división de poderes, pero no, por supuesto, con el enfoque global que dan a esta PNL, porque entendemos que significa favorecer más a los malos que defender a los buenos. **(Aplausos).**

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

Para consumir un turno de fijación de posiciones, tiene la palabra, por el Grupo Mixto, el señor Xuclá,

El señor **XUCLÁ COSTA:** Muchas gracias, señor presidente.

En contra de lo que alguien ha expuesto, creo que es compatible poder apoyar la proposición no de ley del Grupo Socialista, defendida por el señor Luena, y a la vez tomar en consideración elementos muy positivos que plantea la iniciativa del Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, básicamente porque en su punto primero hace una defensa de la importancia del cumplimiento de la Carta de los Derechos Fundamentales, del Convenio Europeo de Derechos Fundamentales y también de la legislación española. Creo que esto es muy importante.

A pesar de esto, señor presidente, pido…, si fuera posible, votación separada del punto número 2 de esta proposición.

El señor **PRESIDENTE:** Es que estábamos en el trámite de ver otra votación separada pedida por otro grupo parlamentario. ¿Podría repetir su petición?

cve: DSCG-12-CM-83

El señor **XUCLÁ COSTA:** Simplemente pido la votación separada del punto número 2.

El señor **PRESIDENTE:** ¿El autor de la proposición tiene algún inconveniente en que se haga votación separada?

El señor **DEL OLMO IBÁÑEZ:** Preferimos que se vote junta toda la proposición.

El señor **PRESIDENTE:** Entonces sí tiene objeción. Para que luego digan que no me entero. **(Risas).** Si quiere puntualizar algo, tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Creo que el debate ha quedado claro. Lo peor que se puede hacer es intentar retorcer los argumentos para conseguir un producto con el que parezca que estás a favor o en contra, en este caso, de los derechos fundamentales de los ciudadanos. Estamos totalmente a favor de los derechos fundamentales, pero de todos los ciudadanos. Por ello, entendemos que Internet debe regularse de forma adecuada para garantizar el anonimato en todos los ámbitos en los que se tiene que garantizar, faltaría más, y la libertad de expresión también. Pero, repito, eso no debe incidir en poder provocar efectos como los que hoy también se están causando sin que haya respuesta cuando sí la habría en el mundo fuera de Internet.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, tiene la palabra el señor Del Olmo. **(Pausa).** Renuncia a ella.

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

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

Algunas veces es jocoso ver como un mismo partido político que denuncia que los partidos clásicos decimos una cosa y hacemos la contraria, unas veces decimos A y otras B, se contradice. Yo solo me tengo que remitir al modelo de Estado y la capacidad de los poderes públicos que defendía Podemos cuando se presentó la alternativa de Pedro Sánchez, cuando el señor Iglesias hablaba de que los altos funcionarios firmasen el apoyo explícito en un documento progubernamental, o lo que era el papel de los jueces de los altos tribunales, o cómo había que poner en marcha políticas de control de los medios de comunicación, privados, por supuesto. Ahora estamos en todo lo contrario, no sé en qué fase estamos del proyecto político de Podemos. Igualmente, esto de poner el título a la iniciativa, una PNL sobre desinformación, y mezclarlo todo, es lo que denuncian que hacen los demás y lo que precisamente practican ellos.

También está lo de buenos y malos. Su opinión es: Aquí están todos los demás, que son los malos, y aquí estamos nosotros, que somos los buenos. Sinceramente, no. Nos gustaría haber votado que sí a tres puntos, porque coincidimos con ellos, y no a otros dos. Lo vamos a argumentar. Es evidente que nos tenemos que basar en hechos que son reales y que elaboran profesionales de este sector que están bastante capacitados. Hay informes múltiples que coinciden en algo, y es en que casi la mitad de la información aproximadamente en el año 2022 va a estar compuesta no de bulos, errores y mentiras, sino de desinformación y noticias falsas con las que de forma intencionada se pretende manipular lo que significan el comportamiento y las opiniones públicas de la sociedad. En este contexto de posverdad, la información falseada de manera intencionada, la realidad alternativa, la distorsión deliberada de la realidad, la manipulación informativa, las mentiras emotivas que no dejan de manejarse en lo que ha sido el clásico campo de la propaganda política propia de los Estados totalitarios, que es la peor acepción de lo que ahora se denominan las relaciones públicas o las estrategias de comunicación, son manejadas como instrumentos de persuasión para la manipulación y el control social. Esa es la desinformación.

¿Qué es lo que se pretende con eso? Si nos vamos a desenvolver en esta sopa de letras de nuevos conceptos, fruto de la práctica y del conocimiento, a incorporar en ese conocimiento la elaboración de una doctrina y de unos principios, porque es algo novedoso, es verdad que también vamos a entrar en la dialéctica propia, que tampoco es nueva, de la libertad de expresión, el derecho de acceso a la información veraz y de calidad o el de la transparencia y la seguridad. Que esto no es nada nuevo es evidente, ya que estaba tanto en la antigüedad como en la Edad Media y en la era moderna en la que se inventa la prensa, los medios de comunicación de masas más actuales, las redes sociales con las TIC, etcétera. A mí me gustaría hacer énfasis en que en este contexto de posverdad, que es el ecosistema de información en el

cve: DSCG-12-CM-83

que nos manejamos actualmente, la noticia falsa es un fiel aliado de la demagogia, una distorsión deliberada de la realidad para manipular la creencia y las emociones, para influir en la opinión pública y en las actitudes sociales, injiriendo en las situaciones internas de otros países, porque es una lucha de unos Estados contra otros por el poder.

Estas informaciones que no se basan en hechos objetivos, sino en la apelación a las emociones, en las creencias, en los deseos de la población o en las necesidades sentidas, no son noticias falsas en el sentido de que sean errores, insultos, comentarios soeces, opinión libre, sino que son informaciones intencionadas, realizadas a través de un sistema de agresión clara y evidente para desestabilizar a los que se consideran adversarios políticos en cuanto a la relación de poder de los distintos Estados en la geopolítica actual o para engrandecer la credibilidad y el poder de quienes las practican, las producen o las originan. De eso estamos hablando cuando nos referimos a la desinformación y a las noticias falsas.

Lo que pretenden los señores de Podemos es que, en vez de reglamentar con el Código de Circulación la libertad de movimientos de los ciudadanos que utilizan un vehículo, nos pongamos en manos de la educación vial solamente. Eso me parece de risa, bastante infantil y propio de la bonhomía en el mundo actual.

Voy finalizando, señor presidente. No podemos dejar correr esto sin organizar una respuesta que regule lo que desde el Grupo Socialista consideramos una de las mayores amenazas actuales para la convivencia y la democracia. Es evidente que lo que pretende esta propaganda es la manipulación de las masas, que tomen conciencia en una etapa determinada de lo que es la vida cotidiana para romper la convivencia, la cohesión social y el crédito de las instituciones.

Finalmente, quiero comentar que si Francia, Italia, Alemania, Estados Unidos, Canadá, Australia, Nueva Zelanda, Japón, todos los países con las democracias más antiguas, que son referentes de la historia de los sistemas democráticos, ponen en marcha iniciativas como las que ya hay contra el terrorismo islamista radical, por qué no vamos a defendernos, que sería la responsabilidad propia de los que legislamos, para garantizar la convivencia de la ciudadanía en nuestro país. Nos parece una renuncia absolutamente infantil.

Finalizo definitivamente comentando —perdón por extenderme otros dos segundos— que nosotros defendemos, en primer lugar, la necesidad de desarrollar un sistema de resiliencia contra esas agresiones y esas amenazas que van más allá de lo que es la simple ciberdelincuencia, del robo de información, porque es muchísimo más grave. En segundo lugar, el refuerzo de la capacidad de respuesta, que es necesaria para poder defendernos, con noticias fundamentadas en hechos reales y no en la desinformación, en la mentira y en la manipulación. En tercer lugar, la definición de nuevos instrumentos reguladores. Yo me pregunto, ¿estaríamos seguros circulando por la vía pública sin un reglamento de circulación? ¿Es posible desenvolverse en el transporte marítimo o aéreo sin los diseños de las rutas de los barcos, de los aviones, de los transportes públicos o de los privados? ¿Sería lógico que los vehículos llevaran matrículas troqueladas o que sus conductores llevaran pasamontañas? Ese planteamiento es un poco sorprendente.

Sin entrar en la máxima contradicción, cómo se puede plantear en un punto reforzar los mecanismos legales existentes para perseguir con mayor eficacia los posibles actos y, por otro lado, entender que los poderes públicos no se pueden mover, encadenarlos y encorsetarlos. No tiene mucho sentido.

Nosotros habíamos solicitado una votación separada, pero nos abstendremos, porque no somos tan malos como dicen los señores de Podemos. Nos hubiera gustado apoyar dos puntos de esta iniciativa y haber votado en contra de otros dos, pero no se nos deja tomar esa decisión libremente.

Nada más. Muchas gracias. **(Aplausos).**

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

Entiendo que la doctrina que ha sentado el señor Del Olmo respecto a la votación separada de las enmiendas de Ciudadanos rige para el Grupo Socialista y que, por tanto, se votará conjuntamente.

Por el Grupo Parlamentario Popular, tiene la palabra el señor Aznar.

El señor **AZNAR FERNÁNDEZ:** Gracias, señor presidente.

Para terminar este debate, y en este clima de cordialidad que preside la Comisión, permítame que le diga en voz alta, señor Del Olmo: ¡Menos mal que están ustedes para recordarnos que tenemos que cumplir la ley! ¡Qué sería de este pobre país si no estuvieran aquí, día a día, para recordar al resto de formaciones políticas que la ley es algo que hay que cumplir!

cve: DSCG-12-CM-83

Le agradezco que nos haya facilitado la votación. Como decía mi colega del Grupo Socialista, nos ha simplificado usted las cuestiones. Con algunas de las cosas que plantean —intentaré exponérselas brevemente— podemos estar de acuerdo, pero tenemos que votar en contra, y no tanto por lo que piden en esos cinco puntos, de los que ahora hablaremos, sino por lo que dicen en la exposición de motivos, que es donde realmente reflejan claramente su pensamiento. Es cierto que las TIC han invadido todos los ámbitos de nuestra sociedad. Es raro que hoy en día exista alguna actividad que no pase por Internet o que no tenga reflejo en las redes sociales, desde la sanidad a la defensa. Estamos de acuerdo en eso. También lo estamos en que junto a esos avances aparecen nuevas vulnerabilidades. Coincidimos en los datos que ustedes aportan, que son del Incibe, que reflejan que esto que estamos diciendo es verdad.

Dicen ustedes en su exposición de motivos —y también lo confirmamos— que España participa en la coalición para la libertad de expresión en Internet. Menos mal que lo reconocen ustedes como una cuestión positiva, porque si no, no sé qué nos estarían pidiendo hoy. De todas formas, aquí empiezan ustedes a asomar la patita —si me permite el símil infantil—. En su proposición se refieren —lo voy a leer textualmente— a que se ha hablado de injerencias extranjeras con el objetivo de desestabilizar España y la Unión Europea mediante ciberataques o campañas de desinformación. Sigo con las comillas. Añaden ustedes: Gran parte de las informaciones y declaraciones de miembros del Gobierno muestran un absoluto desconocimiento de la materia. Sabemos que ustedes están siempre en posesión de la verdad y que lo que decimos los demás no se lo van a creer, aunque lo ratifiquen en el extranjero. Estamos hablando o de puras hipótesis o de planteamientos conspiranoicos, que curiosamente coinciden con las denuncias que se han hecho en Alemania, robo de información de los diputados alemanes, con las que se han hecho en Reino Unido, la señora May advirtiendo claramente a la Unión Soviética, la antigua Rusia, sobre su intento de influencia en el brexit, denuncias en Holanda, en Francia, y no vamos a hablar de Estados Unidos porque lo tenemos cada día en los periódicos. No me resisto a citar que alguna *think tank* americana —está recogido en un periódico de importante tirada nacional— les califica como el caballo de Troya del Kremlin. Sinceramente, creo que exageran en cuanto a sus competencias y posibilidades.

Vayamos, rapidísimamente, señor presidente, uno por uno, a los puntos que ustedes plantean. El punto primero es una obviedad. Decir que las políticas que se establezcan respeten la Carta de los Derechos Fundamentales de la Unión europea, repito que es una obviedad, señorías. Dicen que hay que respetar la Constitución. Creo que para este Gobierno no tiene sentido esa advertencia. Quiero recordarles, sin embargo, que el actual Gobierno ha hecho tres reformas legislativas en la lucha contra la ciberdelincuencia que se basan en el Convenio con la ciberdelincuencia que se aprobó en Budapest en el año 2001, cuya trasposición a nuestro ordenamiento se hizo, si no tengo mal el dato, en el año 2010. Asimismo, se apoyan en la Directiva 2013/40. Por tanto, la Estrategia de Seguridad Nacional, señorías —es su primer punto— está en plena concordancia con la legislación, tanto española como europea.

Punto segundo. El objetivo del Gobierno, contemplado en la Estrategia de Seguridad Nacional de 2017, es garantizar el uso seguro de las redes y de los sistemas de información, fortaleciendo la prevención y la respuesta. Esto que les digo se está haciendo a través de la CERT del Incibe para empresas y ciudadanos, de la CERT de las administraciones públicas y de la CERT del mando conjunto para las redes militares. Quiero recordarles que la identificación de usuario, señorías, está en la competencia de los proveedores de servicios, y el Estado regula las condiciones de identificación de los usuarios.

Punto tercero. Ya hemos hablado de las reformas legales que ha hecho el Gobierno, y no voy a insistir mucho en ellas. Pero sí me gustaría añadir la reforma de los artículos 588 y siguientes de la Ley de Enjuiciamiento Criminal. Entendemos que por el momento no es necesario seguir más allá.

Punto cuarto. Estamos de acuerdo, pero otra vez es una obviedad. La Estrategia de Seguridad Nacional se establece en función de los intereses españoles y de lo establecido en la Unión. Todas las reformas se vienen haciendo con transparencia, como les hemos dicho, y realizando las trasposiciones de la Unión Europea con toda puntualidad.

Terminamos con el punto quinto, que es el que tal vez no hubiéramos apoyado bajo ningún concepto. Si aceptásemos este punto, señorías, estaríamos limitando la capacidad del Gobierno de implementar el objetivo de la Estrategia de Seguridad Nacional 2017, si ello fuera necesario. El Grupo Popular considera que advertir a los internautas de posibles acciones de desinformación o maliciosas y poner a su alcance herramientas que les permitan obtener información veraz, en ningún caso va en detrimento de ninguna libertad individua.

cve: DSCG-12-CM-83

Por ello, señorías, nos oponemos a esta proposición no de ley.
Muchas gracias. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señor Aznar.
Vamos a pasar a las votaciones.
En primer lugar, votamos la proposición no de ley sobre la política de defensa orientada a la prevención de ataques bioterroristas con virus de viruela. Se ha presentado una enmienda transaccional que entiendo que todos los portavoces conocen, por lo que no hace falta leerla.

Efectuada la votación, dijo

El señor **PRESIDENTE:** Queda aprobada por unanimidad.
Enhorabuena, señor Xuclá.
Votamos ahora la proposición no de ley relativa al refuerzo de las capacidades dedicadas a la lucha contra las acciones de desinformación, presentada por el Grupo Parlamentario Socialista. No se han presentado enmiendas.

Efectuada la votación, dio el siguiente resultado: votos a favor, 31; en contra, 5.

El señor **PRESIDENTE:** Queda aprobada.
Doy la enhorabuena al Grupo Socialista.
Votamos la proposición no de ley sobre la elaboración de un Plan de actuación integral para el fomento del empleo en materia de ciberseguridad, presentada por el Grupo Popular. Se vota con la incorporación de la enmienda número 3 de Ciudadanos.

Efectuada la votación, dio el siguiente resultado: votos a favor, 31; abstenciones, 5.

El señor **PRESIDENTE:** Queda aprobada.
Enhorabuena al proponente, que es el Grupo Parlamentario Popular.
Finalmente, votamos la proposición no de ley relativa a la desinformación y su relación con la ciberseguridad en España, presentada por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea. Se vota en sus propios términos al no haber sido aceptada la votación separada.

Efectuada la votación, dio el siguiente resultado: votos a favor, 5; en contra, 20; abstenciones, 11.

El señor **PRESIDENTE:** Queda rechazada.
No puedo felicitarles por el resultado, pero sí por el esfuerzo. **(Risas).**
Se levanta la sesión.

Eran las seis y cinco minutos de la tarde.

cve: DSCG-12-CM-83