



DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2022

XIV LEGISLATURA

Núm. 140

Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DEL EXCMO. SR. D. CARLOS ARAGONÉS
MENDIGUCHÍA

Sesión núm. 15

celebrada el martes, 21 de junio
en el Palacio del Senado

Página

ORDEN DEL DÍA

Debatir.

- **Proposición no de Ley relativa a la mejora de la coordinación del Sistema de Seguridad Nacional en materia de ciberseguridad. (Número de expediente del Senado 663/000053 y número de expediente del Congreso de los Diputados 161/001482).....** 2
Autor: GRUPO PARLAMENTARIO VOX

- **Moción por la que se insta al Gobierno a adoptar medidas urgentes y, en su caso, a tramitar una ley en la que se apruebe un protocolo de actuación que favorezca una coordinación unificada absoluta en la ciberseguridad del ámbito público con el privado, así como a desarrollar una potente red nacional de ciberseguridad para empresas y autónomos. (Número de expediente del Senado 661/001463 y número de expediente del Congreso de los Diputados 161/003711)** 6
Autor: GRUPO PARLAMENTARIO POPULAR EN EL SENADO

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 2

Se abre la sesión a las once horas y cinco minutos.

El señor **PRESIDENTE**: Buenos días, señorías. Se abre la sesión.

En primer lugar, quiero agradecerles su asistencia porque el día no es especialmente el más cómodo para muchos de ustedes. Me han comunicado algunas ausencias, pero creo que no es necesario que se las dé a conocer.

Al término de la sesión, ruego a los portavoces que tengan la amabilidad de permanecer con los miembros de la Mesa para abordar la ponencia de *fakenews*, que la llamamos desinformación.

Insisto en agradecerles su asistencia hoy en el Senado.

DEBATIR.

— **PROPOSICIÓN NO DE LEY RELATIVA A LA MEJORA DE LA COORDINACIÓN DEL SISTEMA DE SEGURIDAD NACIONAL EN MATERIA DE CIBERSEGURIDAD. (Número de expediente del Senado 663/000053 y número de expediente del Congreso de los Diputados 161/001482).**

Autor: **GRUPO PARLAMENTARIO VOX.**

El señor **PRESIDENTE**: Pasamos a la proposición no de ley, presentada por el Grupo Parlamentario Vox. Para su defensa, por un tiempo de cinco a siete minutos, tiene la palabra el señor Utrilla.

El señor **UTRILLA CANO**: Muchas gracias, presidente. Con la venia.

La Ley 36/2015, de Seguridad Nacional, de 28 de septiembre, tiene por objeto coordinar las respuestas ante las amenazas y riesgos a los que se enfrenta nuestro país. Así, en la exposición de motivos de la referida ley, se señala que la seguridad nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos. Esta acción debe seguir unos principios básicos, recogidos en el artículo 4, apartado segundo, de la Ley de Seguridad Nacional. Entre estos, podemos destacar la unidad de acción, la eficiencia, la sostenibilidad de recursos y la coordinación. Asimismo, el artículo 10 de la ley define los ámbitos de especial interés para la seguridad nacional, por resultar básicos para preservar derechos y libertades. Resulta premonitorio que sea la ciberseguridad el primer ámbito que cite esta ley.

En este estado de cosas, nuestro grupo parlamentario presenta esta iniciativa, que tiene como fin desarrollar un programa de atribución que permita ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas, de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz y dar cumplimiento a lo establecido en la Estrategia Nacional de Ciberseguridad de 2019, marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado. Esto facilitaría la identificación de la autoría de los actos o actuaciones en el ciberespacio tipificados como delitos. Asimismo, habría que mejorar la cooperación público-privada en la lucha contra la ciberdelincuencia, y es que esta colaboración público-privada podría marcar un punto de inflexión en la lucha contra el cibercrimen y resultaría clave.

Según información facilitada por Fortinet, las amenazas del primer semestre de 2021 han aumentado significativamente en el volumen y sofisticación de los ataques dirigidos a personas, organizaciones e infraestructuras cada vez más críticas, como los ataques de *ransomware*, *malversiting* y los *botnet*. Aquí cabe destacar lo dispuesto en el quinto capítulo de la Estrategia Nacional de Ciberseguridad, titulado La ciberseguridad en el Sistema de Seguridad Nacional, que define la arquitectura orgánica de la ciberseguridad indicando que, bajo la dirección del presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al presidente del Gobierno en la dirección y coordinación de la política de seguridad nacional en el ámbito de la ciberseguridad y fomenta las relaciones de coordinación, colaboración y cooperación entre administraciones públicas y entre estas y el sector privado, y el Consejo de Situación.

Habría que dotar de mayores recursos al Centro Nacional de Inteligencia, así como potenciar la coordinación a todos los niveles del Sistema de Seguridad Nacional, ampliando el lanzamiento por parte del Centro Criptológico Nacional de un programa piloto de intercambio de información técnica para prevenir ciberincidentes en los que participasen empresas del sector privado y organismos públicos, en el marco del despliegue de la Red Nacional de Centros de Operaciones de Ciberseguridad. Del mismo modo, señorías, España debería potenciar las relaciones con otros Estados y organizaciones

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 3

internacionales y comunitarias en materia de ciberseguridad, como, por ejemplo, la organización de seminarios bilaterales de ciberseguridad. Hace unos meses, España y Estados Unidos organizaron el primer seminario bilateral al objeto de abordar estas cuestiones. El Grupo Parlamentario Vox lo celebra, pero consideramos que queda mucho trabajo por realizar en este sentido. Asimismo, entendemos que, sobre la base de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad, es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional.

Para finalizar, quiero exponer que para combatir todas aquellas ciberamenazas y/o disrupciones o manipulaciones maliciosas o ilícitas que afectan a elementos tecnológicos, habría que promover un ciberentorno seguro y fiable, con el impulso de la creación de empresas privadas nacionales especializadas en el ámbito de la ciberseguridad, entre otras medidas.

En resumen, señorías, el Grupo Parlamentario Vox propone una serie de acciones que resultan coherentes y acordes con nuestro ordenamiento jurídico, y pongo como ejemplo la relativa a la elaboración de un programa de atribución, que es definido como prioridad en la página 27 del Informe Anual de Seguridad Nacional de 2021.

Por todo ello, el Grupo Parlamentario Vox solicita su voto a favor.

Muchas gracias, presidente.

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

El Grupo Popular ha presentado una única enmienda. Tiene la palabra su portavoz, el señor Callejas.

El señor **CALLEJAS CANO**: Muchas gracias, señor presidente. Buenos días, señorías.

Es fundamental considerar la seguridad en el mundo ciber, en toda su extensión, un reto de primer nivel y máxima prioridad en España. Señorías, nos enfrentamos a tres grandes problemas: ciber guerra, ciberespionaje y operaciones de influencia. No exagero cuando afirmo que estamos en una guerra de ámbito global, y cada vez más gente lo percibe porque empieza a afectar a su vida cotidiana con más frecuencia.

El modelo de gobernanza en materia de ciberseguridad presente en España es poco eficiente, carece de recursos humanos y materiales, y lo más grave es que no es único y no está centralizado. Las tres patas que lo componen son: en primer lugar, el CCN-CERT, dependiente del Centro Nacional de Inteligencia, que se centra en el sector público y empresas estratégicas; tiene muy pocos efectivos, pero muy profesionales y realiza una gran colaboración con empresas privadas. En segundo lugar, el Incibe, que depende del Ministerio de Asuntos Económicos y Transformación Digital, y se centra en pymes y en ciudadanos; posee menos experiencia en el sector y tiene la dificultad de que muchas empresas tienen recelos a que los técnicos del Incibe tengan acceso a sus ordenadores, ya que esas empresas tienen sus propios servicios de ciberseguridad; y, en tercer lugar, el ESP DEF CERT, o mando conjunto del ciberespacio del Ministerio de Defensa, que posee un grave problema, y es la gran rotación del personal para poder ascender dentro del ejército; los únicos que permanecen son los reservistas voluntarios.

Como he dicho, el modelo de gobernanza de ciberseguridad nacional no funciona de forma eficaz, hay que ir a un modelo en el que el CCN-CERT incremente los recursos, tanto tecnológicos como humanos y materiales disponibles, para hacer frente a las amenazas descritas anteriormente; todo ello, para hacer frente a la prevención, detección, respuesta, recuperación, investigación y defensa activa. Debemos avanzar hacia un modelo parecido al NCSC, dependiente del Centro Nacional de Ciberseguridad del Reino Unido. Este modelo es el que siguen otros países, como los Países Bajos y Alemania.

El modelo, como digo, que propone el Grupo Parlamentario Popular es que debemos apoyarnos y dotar de recursos y potenciar en España al máximo nuestro CCN-CERT, dependiente del CNI. Hay que tener en cuenta que hay que dotar a este mando único de capacidades defensivas, pero también ofensivas. «No hay mejor defensa que un buen ataque». Esta frase está tomada de la obra *El arte de la guerra*, que suele atribuirse al general, estratega y filósofo chino Sun Tzu, que, supuestamente, vivió hacia el siglo VI antes de Cristo.

Señorías, la ciberseguridad ha de ser transversal en todas las Fuerzas Armadas, como lo es la sanidad. El Grupo Popular propone cuatro posibles acciones: en primer lugar, la creación de un cuerpo como un ciber; en segundo lugar, la creación de una especialidad o arma en ciberdefensa para las Fuerzas Armadas; en tercer lugar, la creación y regulación de la reserva estratégica de talento de ciberseguridad, mediante la captación de reservistas voluntarios, tal y como se aprobó por unanimidad en este Parlamento en la Comisión de Defensa el pasado 21 de abril de 2021, y, en cuarto lugar, explorar la creación de un cuarto ejército: el ejército ciber.

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 4

Señorías, es prioritario también avanzar hacia el concepto de la máxima soberanía ciber. Tanto en la Administración General del Estado como en el resto de las administraciones se deberían evitar los motores de búsqueda cuyos datos puedan ser almacenados y analizados por otros Estados; otra solución sería disponer de un motor de búsqueda propio. Se debería implementar la creación de una nube europea que garantice la confidencialidad de los datos de nuestros ciudadanos y empresas. El Gobierno de España debe incrementar las capacidades del SOC gubernamental, actualmente gestionado por el CCN-CERT. El poder Ejecutivo debe mejorar la coordinación entre el mando conjunto del ciberespacio y el CCN-CERT. Dado que las relaciones económicas son cada vez más digitales, el Gobierno de España también debería crear urgentemente un sistema de inteligencia económica que vele por la seguridad en ese ámbito.

Para finalizar, les comunico que al Grupo Parlamentario Popular le gustaría conocer el criterio del Gobierno de España ante las siguientes cuestiones: ¿Qué opinión posee el departamento de Seguridad Nacional ante la prohibición de instalaciones 5G de los gigantes chinos de las telecomunicaciones Huawei y CTE por parte de los Gobiernos de Estados Unidos y Canadá? También nos gustaría saber por qué España ha quedado en el último lugar en el evento Locked Shields 2022, organizado por el Centro de Excelencia de Ciberdefensa de la OTAN, así como por qué no se han vuelto a publicar los informes anuales de evaluación de la Estrategia Nacional de Ciberseguridad desde 2019.

Esperamos las respuestas. La seguridad nacional depende mucho de ello.

Muchas gracias. **(Varias señorías del Grupo Parlamentario Popular en el Senado golpean repetidamente su mesa con la palma de la mano).**

El señor **PRESIDENTE**: Gracias al enmendante. Su intervención ha sido casi tan extensa como la del proponente, pero una sesión tan interesante como esta de la ciberseguridad se lo merece.

¿Quién desea hacer uso de la palabra en representación de sus grupos para posicionarse? ¿Alguna señoría?

Tiene la palabra el portavoz del Grupo Socialista, don César Mogo Zaro.

El señor **MOGO ZARO**: Disculpeme, presidente, ¿se ha abierto un turno de posición para todos?

El señor **PRESIDENTE**: Respecto de la proposición no de ley, sí.

El señor **MOGO ZARO**: ¿Pero solo intervengo yo?

El señor **PRESIDENTE**: Parece ser que sí.

El señor **MOGO ZARO**: Tendría que ser el último, ¿no?

El señor **PRESIDENTE**: Si solo interviene usted, su señoría puede hacerlo ya.

El señor **MOGO ZARO**: Digo si intervienen más.

El señor **PRESIDENTE**: No, no; no veo a nadie más en el hemiciclo que lo pida, por eso le he dado la palabra.

EL Señor **MOGO ZARO**: Muchas gracias, presidente.

En primer lugar, manifiesto nuestro asombro; no sabía que estábamos en sesión de control al Gobierno. Le informo al diputado de que hoy no cabe preguntar al Gobierno, igual que yo no puedo formular otro tipo de preguntas a la oposición. Por tanto, simplemente quería aclararle su error. Comprendo que era debido a la buena fe, sin duda ninguna, pero hoy no corresponde control al Gobierno. Por tanto, las preguntas quedan formuladas al aire, sin contestar, porque no está el Gobierno.

En segundo lugar, y aclarado este pequeño desliz —comprensible— del portavoz del Grupo Popular **(Rumores)**, quiero decirles que no sé por qué no ha habido turno de respuesta por parte de Vox a la enmienda del Grupo Popular. En todo caso, es lo mismo, porque, señores de Vox...

El señor **PRESIDENTE**: Perdona que le interrumpa.

Tiene razón, lo que pasa es que he entendido que la enmienda era admitida y no lo he comunicado al pleno de la comisión. En todo caso, ya que está en uso de la palabra, no quiero interrumpir, pero si la aclaración del señor Utrilla diera lugar a un tipo de observación por su parte, con mucho gusto le vuelvo a dar la palabra.

Siga el portavoz fijando su posición.

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 5

El señor **MOGO ZARO**: En ese caso, señores de Vox y señores del PP —con la aprobación de su enmienda, por lo que imagino que votarán favorablemente— van a apoyar una moción de lo que no debe hacer el Parlamento, una moción perfectamente prescindible. Sinceramente, les llamo a la reflexión para que antes de finalizar la sesión la retiren. Yo comprendo que ustedes la presentaron en octubre, o algo así, de 2020, pero la realidad les ha desbordado, carece de sentido. Se lo digo con toda la honestidad, comprendo que no les agrada porque no es agradable retirar una enmienda, pero así le evitarían también al Partido Popular el trago de tener que apoyar una moción que es perfectamente prescindible. ¿Por qué es prescindible? Porque la realidad los ha desbordado.

En política, debemos valorar las cosas como son, más allá de las diferencias ideológicas, y apelar a ese sentido que tanto nos reclaman los ciudadanos, que es el sentido común, y no aprobar una moción que ha sido desbordada por la realidad. Porque, aparte de alguna generalidad que otra, como potenciar relaciones con otros Estados y otras organizaciones —¿creen de verdad que los instrumentos, mecanismos y organismos de ciberseguridad en España no potencian las relaciones con otros Estados? Estaríamos buenos si no lo hicieran, pues claro que lo hacen—, o el incremento de recursos al Centro Nacional de Inteligencia, que es un clásico... Y es que, además, las medidas del Plan de medidas de respuesta a la guerra conllevan una partida presupuestaria de 1200 millones de euros en materia de ciberseguridad. Ustedes no lo votan, lo sé, tampoco deben estar a favor de ese incremento de recursos en materia de seguridad porque lo rechazan, pero es un dato importante de lo que ha sucedido en este tiempo.

En segundo lugar, hay muchas cuestiones de las que ustedes plantean que ya están hechas con otros nombres. Por ejemplo, se ha creado una plataforma de seguimiento de ciberseguridad mediante un real decreto del año 2021, o un plan estratégico contra ciberataques, que es lo que ustedes plantean, pero con otros términos; la Policía Nacional ha creado una división de operaciones en materia de ciberseguridad, otro ejemplo de cuestiones que se han ido creado en este tiempo.

En marzo de 2022 se creó el Plan Nacional de Seguridad, que es la respuesta a un mandato del Consejo de Seguridad Nacional y el desarrollo de la Estrategia de Seguridad Nacional, que dedica una parte esencial a dejar claras las líneas en materia de ciberataques y contempla más de cien actuaciones, entre ellas, la creación de un sistema integrado de ciberseguridad; la creación del centro de operaciones —se está en ello— de seguridad de la Administración General del Estado; una plataforma de notificaciones y seguimiento de ciberincidentes y también de amenazas... En fin, hay dotación de recursos económicos, hay creación de instrumentos de defensa ante los ciberataques, como no puede ser de otro modo, porque el diagnóstico ante el incremento y ante el riesgo que suponen los ciberataques está muy presente entre todos nosotros —creo que en esto sí coincidiremos—. Pero es que la Estrategia de Seguridad Nacional, posterior también a su moción de 2021, planteaba toda una serie de elementos que tenían que ver con el ciberespacio y contra los sistemas tecnológicos que utilizan los ciberataques.

Por tanto, desde la PNL en adelante se ha producido un avance, un desarrollo institucional en la lucha contra los ciberataques que, sinceramente y dicho con todo respeto, son cosas que nos pasan a todos parlamentariamente, la dejan en desuso por completo.

Voy acabando, señor presidente. Quiero referirme también a que aquí hay miembros de la Asamblea Parlamentaria de la OTAN y saben que, para mayor añadidura, en la Cumbre de Madrid se va a elaborar el concepto estratégico y las iniciativas 2030, va a haber una serie de desarrollos y se van a aprobar cuestiones en materia de ciberataques y de lucha contra los ciberataques. La OTAN viene desarrollando su estrategia desde 2002 y ahora, en 2022, culminaremos con un desarrollo importante en materia de lucha contra los ciberataques.

Acabo ya, definitivamente. Ustedes están en su libertad de presentar los materiales que consideren necesarios y llevar adelante la moción, pero, como he dicho, la moción ha quedado desfasada en el tiempo. Van ustedes a votar, y los señores del Partido Popular probablemente también, una moción cuyos desarrollos han quedado completamente desfasados. Ustedes son muy libres de hacer lo que quieran, pero creo que la realidad ha desbordado las expectativas de la PNL, que no digo que no fueran incluso bien intencionadas.

Muchas gracias, señor presidente. **(Varias señorías del Grupo Parlamentario Socialista golpean repetidamente su mesa con la palma de la mano).**

El señor **PRESIDENTE**: Gracias, senador Mogo.

¿Desea el señor Utrilla hacer algún comentario a la Comisión a propósito de la enmienda?

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 6

El señor **UTRILLA CANO**: Sí, gracias, presidente.
Aceptaremos la enmienda presentada por el Grupo Popular.

El señor **PRESIDENTE**: Gracias.

Es bueno no solo que en la Mesa lo sepamos —y me corrijo a mí mismo—, sino que el pleno de la comisión conozca cómo va en cuanto a la aceptación de una iniciativa presentada.

Muchas gracias.

— **MOCIÓN POR LA QUE SE INSTA AL GOBIERNO A ADOPTAR MEDIDAS URGENTES Y, EN SU CASO, A TRAMITAR UNA LEY EN LA QUE SE APRUEBE UN PROTOCOLO DE ACTUACIÓN QUE FAVOREZCA UNA COORDINACIÓN UNIFICADA ABSOLUTA EN LA CIBERSEGURIDAD DEL ÁMBITO PÚBLICO CON EL PRIVADO, ASÍ COMO A DESARROLLAR UNA POTENTE RED NACIONAL DE CIBERSEGURIDAD PARA EMPRESAS Y AUTÓNOMOS. (Número de expediente del Senado 661/001463 y número de expediente del Congreso de los Diputados 161/003711).**

Autor: **GRUPO PARLAMENTARIO POPULAR EN EL SENADO.**

El señor presidente lee el título que figura en el orden del día.

El señor **PRESIDENTE**: Para la defensa de la moción, tiene la palabra el senador Márquez.

El señor **MÁRQUEZ SÁNCHEZ**: Muchas gracias, señor presidente.

Aunque no esté aquí el Gobierno, obviamente, todos los que estamos presentes tenemos derecho a formular las cuestiones que estimemos oportunas, máxime cuando simplemente estamos preguntando; o sea, esa posibilidad siempre existe. **(Rumores).**

En cuanto al tema en concreto, hemos realizado una transaccional —y lo quiero agradecer a los partidos que la han suscrito— sobre la parte dispositiva de la presente moción. Creo que, en el fondo, es una preocupación que tenemos todos: hay un mercado al alza de los datos personales que existen en internet, que se obtienen de las actividades y gestiones que realizamos todos, y las grandes plataformas cogen ese tipo de datos para hacer un *marketing* digital personalizado y ofrecer productos muy concretos a esas personas. Esa es la huella digital que dejamos y las plataformas predicen con ella las conductas de las personas.

Este es un tema sobre el que tenemos que estar siempre atentos. Hay que estar abiertos a la tecnología, por supuesto, pero también hay que ver los riesgos que puede producir su uso, porque las empresas tecnológicas, hablamos de las grandes plataformas, tienen un conocimiento perfecto sobre nosotros, sobre nuestras conductas y, obviamente, sobre nuestros hábitos, gustos, y, por tanto, son unos datos personales que, como decía el presidente de Telefónica, corresponden a la dignidad de las personas. Es un tema lo bastante importante y no puede ser que los datos circulen libremente, incluso siendo objeto de comercio. Estos datos suelen ser objeto muchas veces de ataques por los delincuentes, ciberataques utilizando la tecnología *botnet*, que se traducen concretamente en ilícitos penales: acoso digital a las personas; suplantar la identidad digital; falsificación de perfiles digitales; amenazas o injurias a un tercer usuario; actuaciones constitutivas de violencia de género, que también existen; difusión de datos protegidos que pueden afectar a la salud; robo de los datos de cuentas bancarias, de la Seguridad Social; ataques como el que hemos visto en esta legislatura al SEPE, realizados, probablemente, por bandas de origen cercano a Rusia; estafas; robos de datos personales, etcétera. Es decir, es un tema con el que debemos tener especial precaución, especialmente en el estado geopolítico que estamos viviendo actualmente.

Nosotros, obviamente, damos mucha importancia a la protección de datos del sector público, pero el sector privado también debe tener especial sensibilidad a la protección de los datos de las personas. ¿Por qué? Porque a lo mejor el Estado sí está protegiendo los datos de los ciudadanos, pero si es una empresa privada sensible, que tiene muchos datos de muchas personas, la que recibe un ciberataque, quizá se esté produciendo un boquete dentro de la seguridad nacional, y esas cuestiones también hay que controlarlas. Pero en estos casos el riesgo que produce es doble. Cuando una empresa privada recibe un ciberataque de esta naturaleza, el primer cliente del ciberdelincuente está claro quién es, la misma empresa a la que han robado, porque es la primera que va a querer pagar para recuperar los datos que le han robado y, sobre todo, por una cuestión de prestigio, ya que no quieren que nadie se entere de que esos datos se han robado. Pero, desde el punto de vista de la seguridad nacional, el problema está en que

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 7

ese dinero puede servir para la comisión de delitos, obviamente, y, por tanto, es una cuestión en la que tenemos que estar encima, además de que los datos están, podríamos decir, en manos de cualquiera.

Por eso, es importante que haya una coordinación absoluta entre el Estado y el sector privado. Obviamente, hay que respetarlo y el sector privado tendrá su opinión sobre qué medidas se tienen que tomar a nivel de seguridad, pero la última palabra la debe tener el Estado. O sea, las autoridades de la seguridad nacional tienen que tener la última palabra para una mejor coordinación, sobre todo porque es en beneficio de todos y porque la confianza, tanto del sector público como del sector privado —además de que, muchas veces, la financiación e inteligencia de sector privado es más avanzada que la del sector público—, puede servir de complemento para que exista una perfecta coordinación entre todos y evitar este tipo de riesgos, que, vuelvo a decir, no solamente son fugas de datos de españoles en este caso concreto, sino que también es dinero que va destinado a la comisión de otros delitos.

Hemos realizado una transaccional con el PSOE, que les quiero agradecer, y también Vox ha hecho un esfuerzo en este sentido. A continuación, se la pasaremos a la Mesa.

Muchas gracias. **(Aplausos en los escaños del Grupo Parlamentario Popular en el Senado).**

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

Hay una enmienda presentada por el Grupo Parlamentario Socialista. Tiene la palabra la diputada Retuerto.

La señora **RETUERTO RODRÍGUEZ**: Gracias, presidente.

Hemos presentado una enmienda en la que recogemos que los temas de ciberseguridad ya se están trabajando en el departamento de Seguridad Nacional. Es uno de los grandes e importantes desafíos en la era digital, por la dispersividad y la difícil trazabilidad, sin claras fronteras jurisdiccionales, que nos muestran la fragilidad y la magnitud de la vulnerabilidad a la que las amenazas nos someten constantemente y que suponen un verdadero riesgo al que debemos hacer frente desde las instituciones desarrollando técnicas tanto privadas como públicas.

En ese sentido, hemos trabajado con el senador del Partido Popular autor de la moción para presentar una transaccional, en la que recogemos las iniciativas que el Gobierno de España ya está llevando a cabo en materia de ciberdelincuencia y ciberseguridad y en la que se tienen en cuenta las diferentes directivas de la Unión Europea que se han traspuesto a nuestro ordenamiento jurídico español, concretamente con el Decreto Ley 12/2018, que está considerada además como la primera legislación horizontal en materia de ciberseguridad en España.

Por tanto, ruego tenga en cuenta la Mesa la transaccional.

Muchas gracias. **(Aplausos en los escaños del Grupo Parlamentario Socialista).**

El señor **PRESIDENTE**: Con mucho gusto la tendremos en cuenta.

¿La transaccional está dispuesta? **(Pausa).**

¿Quiere algún senador o diputado miembro de la comisión hacer uso de la palabra?

Tiene la palabra el señor Utrilla, por el Grupo Parlamentario Vox.

El señor **UTRILLA CANO**: Muchas gracias, presidente.

La iniciativa que plantea el Partido Popular insta al Gobierno a adoptar medidas urgentes, en su caso a tramitar una ley que apruebe el protocolo de actuación que favorezca la coordinación unificada absoluta tanto en la ciberseguridad del ámbito público como en el privado, así como a desarrollar una potente red nacional de ciberseguridad para empresas y autónomos.

El objeto de esta moción es la aprobación de un protocolo de actuación que favorezca una coordinación unificada, pero también insta al Gobierno a que emita un informe a esta comisión sobre esta materia y al desarrollo también de una red nacional de ciberseguridad para empresas y autónomos, en el futuro de la cultura de la ciberseguridad. Algo muy parecido pudimos comprobar algunos de los miembros de esta comisión en Estonia, cuando estuvimos allí de viaje con el curso Cesedén: cómo un pequeño país, de 1 300 000 habitantes, se ha convertido en una potencia mundial de ciberseguridad gracias al impulso estatal y, sobre todo, a esa coordinación centralizada y a la colaboración público-privada.

Así las cosas, esta iniciativa es acorde con los planteamientos que se han realizado por mi grupo parlamentario Vox en esta comisión y haré hincapié en que uno de los puntos que nosotros defendemos también es acorde con la iniciativa que hemos presentado hoy aquí. Este refuerzo de la coordinación supondrá una potenciación de la capacidad de gestión del Estado central frente a las comunidades, lo cual

DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Núm. 140

21 de junio de 2022

Pág. 8

nos parece esencial para aumentar la eficacia y la solvencia a nivel nación, y poder dar una respuesta más rápida y concertada en cualquier punto de nuestro país.

Consideramos que esta iniciativa se complementa perfectamente con la que ha presentado hoy mismo nuestro grupo y que en algunos puntos es casi concurrente, así que daremos nuestro voto a favor.

Muchas gracias. **(Aplausos)**.

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

No hay ninguna otra intervención solicitada.

Como me sugiere la letrada, vamos a suspender la sesión por unos minutos para fotocopiar el texto y que lo puedan conocer todas sus señorías. No más de cinco minutos.

Se suspende la sesión a las once horas y treinta y seis minutos.

Se reanuda la sesión a las once horas y cuarenta y tres minutos.

El señor **PRESIDENTE**: Si les parece a sus señorías, comenzamos.

¿Disponen ya del texto de la transaccional que nos ocupaba? **(Pausa)**.

No hace falta que lo lea, ¿verdad? **(Pausa)**.

— **PROPOSICIÓN NO DE LEY RELATIVA A LA MEJORA DE LA COORDINACIÓN DEL SISTEMA DE SEGURIDAD NACIONAL EN MATERIA DE CIBERSEGURIDAD.—Votación. (Número de expediente del Senado 663/000053 y número de expediente del Congreso de los Diputados 161/001482).**

Autor: **GRUPO PARLAMENTARIO VOX.**

El señor presidente lee el título que figura en el orden del día.

El señor **PRESIDENTE**: Vamos a proceder a la votación de la moción con la inclusión de la enmienda del Grupo Popular.

Efectuada la votación, dio el siguiente resultado: votos a favor, 15; en contra, 17.

El señor **PRESIDENTE**: Ha sido rechazada.

— **MOCIÓN POR LA QUE SE INSTA AL GOBIERNO A ADOPTAR MEDIDAS URGENTES Y, EN SU CASO, A TRAMITAR UNA LEY EN LA QUE SE APRUEBE UN PROTOCOLO DE ACTUACIÓN QUE FAVOREZCA UNA COORDINACIÓN UNIFICADA ABSOLUTA EN LA CIBERSEGURIDAD DEL ÁMBITO PÚBLICO CON EL PRIVADO, ASÍ COMO A DESARROLLAR UNA POTENTE RED NACIONAL DE CIBERSEGURIDAD PARA EMPRESAS Y AUTÓNOMOS.—Votación. (Número de expediente del Senado 661/001463 y número de expediente del Congreso de los Diputados 161/003711).**

Autor: **GRUPO PARLAMENTARIO POPULAR EN EL SENADO.**

El señor presidente lee el título que figura en el orden del día.

El señor **PRESIDENTE**: Votamos la moción en los términos transados.

Efectuada la votación, dio el siguiente resultado: votos a favor, 31; abstenciones, 1.

El señor **PRESIDENTE**: Queda aprobada.

Se levanta la sesión.

Eran las once horas y cincuenta minutos.

cve: DSCG-14-CM-140