DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2024 | XV LEGISLATURA | Núm. 43 | Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DE LA EXCMA. SRA. D.ª EDURNE URIARTE BENGOECHEA

Sesión núm. 5

celebrada el jueves 19 de septiembre de 2024 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

Debate y votación de la siguiente propuesta de creación de ponencia:

---

cve: DSCG-15-CM-43

Se abre la sesión a las nueve de la mañana.

DEBATE Y VOTACIÓN DE LA SIGUIENTE PROPUESTA DE CREACIÓN DE PONENCIA:

— DE ANÁLISIS DE LAS AMENAZAS EN EL CIBERESPACIO, EN LA ERA DE LA INTELIGENCIA ARTIFICIAL Y LA COMPUTACIÓN CUÁNTICA, PARA LA ELABORACIÓN DE UN INFORME DE RIESGOS Y RECOMENDACIONES DE MEJORA. A PETICIÓN DEL GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO. (Número de expediente del Congreso de los Diputados 158/000008 y número de expediente del Senado 573/000002).

La señora **PRESIDENTA:** Buenos días a todos. Vamos a dar comienzo a la primera sesión, en este periodo de sesiones, de la Comisión Mixta de Seguridad Nacional, con un único punto del orden del día, que es el debate y votación de la siguiente propuesta de creación de la ponencia llamada de análisis de las amenazas en el ciberespacio, en la era de la inteligencia artificial y la computación cuántica, para la elaboración de un informe de riesgos y recomendaciones de mejora.

Les recuerdo que la Mesa, en su reunión del pasado 17 de septiembre, acordó que el debate se sustancie de la siguiente manera. En primer lugar, intervendrá el grupo autor de la iniciativa por un tiempo de cinco minutos y, a continuación, el resto de grupos, en orden de mayor a menor, también por un tiempo de cinco minutos.

En primer lugar, por lo tanto, en nombre del Grupo Parlamentario Popular, autor de la iniciativa, interviene don Mario Cortés.

El señor **CORTÉS CARBALLO:** Buenos días, señorías.

Todos somos conscientes de que el avance de la digitalización en todos los ámbitos de la sociedad ha supuesto un indudable progreso tanto en productividad como en desarrollo económico, bienestar social y bienestar ciudadano, pero eso también ha provocado que ahora tengamos nuevos frentes que proteger para garantizar la seguridad de nuestra nación. Todos los Gobiernos están desarrollando con mayor o menor acierto estrategias y programas de ciberseguridad para proteger a sus ciudadanos, empresas, infraestructuras y procesos electorales, así como los propios valores democráticos de los países occidentales.

En los conflictos que estamos viendo actualmente, como, por ejemplo, la invasión rusa de Ucrania, estamos experimentando que las guerras ya empiezan a ser híbridas. Por un lado, hay una parte de ciberataques que buscan mermar las capacidades de defensa del país y sus infraestructuras, provocar el miedo en la población y alterar, al fin y al cabo, su vida cotidiana; por otro lado, está el ciberespionaje, que viene a robar documentación crítica de esos países; y, por otra parte, y no menor, está lo que se llama el hacktivismo *hacker,* que viene a atacar medios de comunicación y organizaciones para lanzar mensajes ideológicos y, de esa manera, establecer algún tipo de cambio social en el propio país. Todos estos son los retos a los que nos estamos enfrentando.

España ha utilizado los fondos Next Generation para financiar su estrategia de ciberseguridad, aunque de forma poco eficiente, con evidentes duplicidades y faltas de coordinación. Sin embargo, los datos nos obligan a analizar en profundidad las políticas y las acciones que este Gobierno está ejecutando. En los últimos seis meses, empresas y entidades públicas han afrontado un promedio de 1133 ataques semanales. Los casos denunciados se dispararon hasta los 470 400 en el año 2023. Hay que tener en cuenta que no todos los ataques que tienen éxito se denuncian, pues, por ejemplo, en muchas ocasiones, en los ataques de secuestro de información se paga la información y no se denuncia por miedo a la reputación de la empresa; y también se producen muchos robos de información en los que ni siquiera el propio afectado es consciente de que ha sufrido un ataque su empresa o de que tiene un programa de espionaje dentro de sus propios sistemas. Por lo tanto, a esos 470 400 casos, que nos parecen ya alarmantes, hay que sumar un porcentaje aún mayor de casos que no se denuncian y otros que ni siquiera se conocen.

Todo este aumento entendemos que se produce por varios motivos. Por un lado, la inestabilidad internacional, como ya hemos dicho: la invasión rusa de Ucrania, el conflicto israelí-palestino, la guerra comercial con China o la continua amenaza del yihadismo, pues todo eso es un caldo de cultivo para potenciar este tipo de ataques. También, cada vez es mayor la profesionalización de las organizaciones criminales, que cada vez cuentan con más medios y sofisticación en sus ataques. Por otro lado, hay un aspecto crucial, y es el principal motivo de que estemos aquí hoy, que es la generalización del uso de

cve: DSCG-15-CM-43

inteligencia artificial generativa como herramienta para potenciar los ataques de ciberseguridad. Estas herramientas permiten, por ejemplo, la creación automática de códigos malignos para los ataques, por lo que ya no hace falta ningún informático especializado, pues directamente estos programas, como ChatGPT, etcétera, serían capaces de generar el código maligno, el *malware,* para atacar cualquier institución; y además permiten la automatización y la sofisticación en los ataques, y hacerlo de forma masiva y coordinada. Y en otros casos, hemos visto cómo permiten la manipulación de voz, vídeos o imágenes, que después se usan para los ciberdelitos, para socavar procesos electorales o difundir pensamientos políticos y religiosos para desestabilizar nuestra democracia y la confianza en las instituciones. Tenemos muchos casos en los que se suplanta la identidad tras modificar la imagen de las caras de los vídeos o la voz, para que parezca que la llamada la hace una persona u otra. De hecho, el 40 % de este aumento de ciberataques se debe al uso de estas nuevas herramientas de inteligencia artificial.

Por último, aunque no está dentro del alcance de las organizaciones criminales de momento por el alto coste que supone, tenemos la aparición de la computación cuántica. Hoy en día, los ordenadores cuánticos son infraestructuras muy costosas que no están al alcance de estos criminales, pero sí al alcance de otros gobiernos y, por tanto, tiene que empezar a preocuparnos. La computación cuántica tiene muchos beneficios, sin embargo, también supone un riesgo si se usa de manera malintencionada. Va a suponer una amenaza real para los sistemas criptográficos, para las claves de seguridad y la encriptación de los datos. Cualquier sistema de clave cifrada, desde el comercio electrónico hasta la banca *online,* pasando por sistemas de acceso a *e-mails* de empresas, o simplemente la firma electrónica para la Administración pública, está en riesgo, ya que un ordenador cuántico puede descifrarla en cuestión de segundos. Por un lado, se cree que ya hay Gobiernos que están almacenando masivamente datos y comunicaciones críticas, que han sido interceptadas, con la idea de que, en breve, la potencia de computación de estos ordenadores será capaz de descifrarlas. Imaginen ustedes lo que supone para la seguridad nacional de un país que sus mensajes e informaciones encriptadas puedan ser desencriptados en los próximos meses y, por tanto, poner en total riesgo todas las infraestructuras, planes y estrategias de seguridad que tenga cada uno de los países. Y, por otro lado, es tal la preocupación que ha supuesto este tema de la computación cuántica que el Senado de los Estados Unidos ya en el año 2022 —nosotros vamos un poco tarde— aprobó por unanimidad —curioso, pues en los Estados Unidos la unanimidad está siendo complicada en los últimos años— un acuerdo para establecer una ley que abordara el problema de seguridad que supondrá la computación cuántica para las infraestructuras norteamericanas.

La Comisión Europea ha advertido de ciberataques más complejos y sofisticados y el intento de injerencias de potencias extranjeras, y ha aprobado...

La señora **PRESIDENTA:** Tiene que ir terminando, señor Cortés.

El señor **CORTÉS CARBALLO:** ... la Directiva NIS2, que precisamente viene de la Unión Europea para intentar abordar esta situación.

Como ven, señorías, es necesario evaluar todas estas nuevas amenazas a través de esta ponencia que, de la mano de expertos del sector público y privado, nos permitirá definir los cambios legislativos y las acciones para mejorar nuestras capacidades de defensa.

Muchísimas gracias. **(Aplausos).**

La señora **PRESIDENTA:** A continuación, intervendrán los portavoces del resto de grupos parlamentarios, de mayor a menor.

En primer lugar, por el Grupo Parlamentario Socialista, tiene la palabra don Víctor Javier Ruiz De Diego.

El señor **RUIZ DE DIEGO:** Muchas gracias, señora presidenta.

Buenos días, señorías.

Nos encontramos ante un tema interesante, importante y de gran trascendencia para nuestro país y para nuestra seguridad y anunciamos, en nombre del Grupo Parlamentario Socialista, nuestro voto favorable a la propuesta, creo que con alguna enmienda que luego será objeto de aclaración de cómo quedará el texto de la resolución que va a ser objeto de votación.

Señorías, la capacidad de los Estados para hacer frente a los retos que plantea la ciberseguridad es un elemento estratégico y de primer orden, tanto para protegerse como para progresar en el complejo

cve: DSCG-15-CM-43

panorama geopolítico actual. Así, en un contexto de amenazas cada vez más complejas y en ocasiones difíciles de detectar, resulta más que necesaria la formación en y de las organizaciones que se mueven en este mundo, sean la Administración Pública o algunas del sector privado, con el fin de difundir la conciencia sobre las amenazas en el ciberespacio.

Consideramos en el Grupo Parlamentario Socialista que también es básico trabajar e incidir sobre la tan necesaria conciencia relativa a la seguridad de la información, pues nos afecta a todos y no solo a unos pocos que trabajen o usen sus servicios. Y es que hemos de ser conscientes todos del uso y efectos que la inteligencia artificial puede tener en la prestación de servicios a los ciudadanos. En España, ya hay diferentes organismos e instituciones que tratan de una manera u otra con tales asuntos, tanto en el ámbito civil como en el militar, pero no solo que actúen frente a las situaciones relativas al ciberespacio, sino que es también vital que haya un estudio y una formación continua en este sentido. Así, debemos recordar que el Mando Conjunto del Ciberespacio es el órgano responsable del planeamiento, dirección, coordinación, control y ejecución de las acciones tendentes a asegurar la libertad de acción de las Fuerzas Armadas en el ciberespacio. En otras palabras, se encarga de la ciberdefensa; y para cumplir su misión planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio, atendiendo los planes operativos en vigor.

Por otro lado, tenemos el Centro Criptológico Nacional, creado en el año 2006 por un Gobierno socialista y adscrito al Centro Nacional de Inteligencia, cuya misión es la de contribuir a la mejora de la ciberseguridad española. Es, pues, el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques, además de afrontar de forma activa las diferentes ciberamenazas que se produzcan, incluyendo la coordinación a nivel público estatal de las distintas capacidades de respuesta a incidentes de centros de operaciones de ciberseguridad existentes. Además, busca fomentar, desarrollar y mantener perfiles profesionales cualificados frente a las ciberamenazas, contribuyendo en todos los niveles —dirección, gestión, implantación y usuarios— a un cambio de paradigma educativo basado en un aprendizaje permanente como potencial fuerza laboral. El centro tiene entre sus funciones la de formar al personal de las administraciones públicas españolas a través de un amplio programa de cursos, y en el desarrollo de su actividad —en dicha búsqueda de talento—, el centro ha desarrollado la plataforma ATENEA, una plataforma en la que podemos comprobar nuestros conocimientos y destrezas ante problemas de criptografía y esteganografía forense, análisis de tráfico, *reversing, hacking web,* etcétera. Esta herramienta busca concienciar al personal relacionado con las TIC sobre los riesgos existentes en este campo. Se trata de una magnífica estrategia para buscar e involucrar a profesionales con experiencia en ciberseguridad, con el fin de que puedan demostrar sus habilidades y capacidad en materia de ciberseguridad. Una prueba del éxito de dichas acciones son los más de 11 000 usuarios registrados, así como los numerosos retos publicados.

Otra de las actividades del Centro Criptológico que nos gustaría poner en valor son las jornadas de talleres eminentemente prácticos, cuyo objetivo no es otro que el de fomentar la especialización en conocimientos técnicos impartidos por profesionales y expertos del sector a través de clases eminentemente prácticas sobre ámbitos relacionados con la ciberseguridad, la seguridad TIC, respuestas a incidentes, ciberinteligencia y seguridad operacional. En ellos participan profesionales de la ciberseguridad con sus equipos portátiles para llevar a cabo los ejercicios planteados y, de este modo, queda meridianamente claro que el factor humano tiene una importancia vital, como no podía ser de otra manera, en este tipo de estrategias y acciones. No olvidemos que para protegerse y actuar con relativo éxito frente a las amenazas y retos de las ciberamenazas y del ciberespacio es vital el fomento, desarrollo y mantenimiento de perfiles profesionales cualificados en todos los niveles: la dirección, la gestión, la implantación y los usuarios.

No podemos dejar de citar, en último lugar, al Instituto Nacional de Ciberseguridad, el INCIBE, una empresa pública española organizada como sociedad anónima propiedad del Ministerio para la Transformación Digital y de la Función Pública, entre cuyas funciones cabe destacar el soporte que en materia de seguridad informática ofrece a ciudadanos, empresas públicas y privadas, así como a las administraciones públicas y sus organismos, a las instituciones académicas y de investigación y, especialmente, aquellas que gestionan infraestructuras críticas. Debemos recordar que el INCIBE participa en la Estrategia Nacional de Ciberseguridad. Y por lo que respecta al sector privado y al universitario, hay excelentes profesionales que bien pueden apoyarnos y colaborar con esta labor que en breve comenzaremos.

cve: DSCG-15-CM-43

Los trabajos de esta ponencia deberían materializarse conforme a una serie de criterios que aseguren su eficacia y eficiencia, y que había que definir entre todos los grupos que conforman la Comisión. Señorías, para este Gobierno, para nosotros los socialistas, la búsqueda de talento y soluciones en ciberseguridad es un elemento crítico.

Muchas gracias. **(Aplausos).**

La señora **PRESIDENTA:** A continuación, por el Grupo Parlamentario VOX y Grupo Parlamentario Mixto en el Senado, tiene la palabra don Alberto Asarta.

El señor **ASARTA CUEVAS:** Buenos días.

En la última reunión que tuvimos de Mesa y portavoces se comentó la creación, reglas de funcionamiento y composición de esta Ponencia que hoy vamos a aprobar casi con toda seguridad. Hoy hemos recibido este documento ya actualizado, al cual, leyéndolo con tranquilidad, no hay nada que objetar. Lo importante de todo esto es que en esta ponencia se elabore un informe de riesgos y recomendaciones de mejoras cuando terminemos, que se ha ampliado a dos sesiones más, por lo que me han contado y aparece por aquí.

Hay poco que añadir al discurso del ponente del Grupo Parlamentario Popular. Solamente piensen que si en el ámbito de la guerra electrónica, que está uno o dos escalones por debajo de lo que es la ciberdefensa o el ciberespacio, si en ese ámbito de la guerra electrónica acabamos de ver de dos días para acá lo que Israel es capaz de hacer con los buscas de personas o con los *walkie-talkies,* imagínense qué no se podrá hacer con la inteligencia artificial y con la computación cuántica.

Consideramos que esto es una exigencia de nuestra sociedad, una exigencia para proporcionar seguridad a nuestros ciudadanos. La misión fundamental y principal de cualquier Gobierno de cualquier país del mundo es la protección de sus ciudadanos, y mi grupo considera que es fundamental que esta ponencia que vamos a aprobar en la Comisión Mixta de Seguridad Nacional trabaje en coordinación con la Comisión de Defensa. Casualmente hoy, cuando termine esta Comisión, tenemos también Comisión de Defensa, y se va a tratar un tema muy importante, que es la creación de una reserva de talento referente a ciberseguridad, que trabajará en estrecha coordinación con el mando de ciberdefensa que tenemos ya previsto y creado en España. Me gustaría, aprovechando que tengo tiempo, comentarles un poco la creación de esta reserva estratégica de talento en ciberseguridad, que tiene como fin disponer de recursos humanos con los que reforzar los medios permanentes del Ministerio de Defensa en apoyo de sus necesidades dentro del ámbito específico de la ciberdefensa, o para hacer frente a situaciones que afecten a la seguridad nacional. Todos estamos totalmente implicados en esto. Esta reserva estratégica de talento en ciberseguridad tendrá por objeto incorporar capacidades, conocimientos y habilidades aplicables al ciberespacio de los ciudadanos que voluntariamente decidan colaborar en cumplimiento del interés general de incrementar el nivel de ciberseguridad. Hoy habrá una proposición no de ley del Grupo Popular que espero, además, que también salga adelante, porque es muy necesaria para España.

Así que nada más que añadir a este asunto. Sí quiero insistir en que es fundamental y necesario —si queremos estar a la cabeza, tener voz y que se nos oiga en el mundo en el tema de la ciberdefensa— echar muchos arrestos, mucho tiempo y mucho trabajo para que esto vaya adelante y vaya bien, que es lo fundamental.

Nada más. Muchas gracias.

La señora **PRESIDENTA:** A continuación, por los grupos parlamentarios Plurinacional SUMAR e Izquierda Confederal, tiene la palabra don Félix Alonso.

El señor **ALONSO CANTORNÉ:** Gracias, presidenta. Gracias por recortar el nombre, porque es muy largo.

Buenos días.

Hace unos meses salió un titular en un medio de comunicación serio, no en un seudomedio, que nos sorprendía un poco — supongo que a algunos, a otros no— que decía: El 1 % más rico de España disparó sus rentas tras la pandemia y aumentó la distancia con el resto de las clases sociales. Los hogares más adinerados son los que más han aumentado su renta entre 2017 y 2021, un 43 %. Estas personas contribuyeron menos a la tributación de lo que les correspondía por renta, 189 276 hogares son el 1 % del total existente en España, acumularon el 10,5 % de la renta del mercado en el año 2021. ¿A qué viene esto? A que el conocimiento científico y los desarrollos tecnológicos derivados tienden siempre a ser

cve: DSCG-15-CM-43

controlados por y para beneficiar a algunos grupos sociales determinados —ese 1 % es el que paga menos; es incomprensible siendo el resto el 99 %—, quedando al margen el resto de la población.

A lo largo de la historia, los actores más influyentes han utilizado el engaño para aumentar su poder. Las empresas de inteligencia artificial están en una carrera sin control para crear una inteligencia artificial superinteligente, valga la redundancia, que supere a los humanos en la mayoría de las capacidades económicas y estratégicamente relevantes. Una inteligencia artificial de este tipo sería experta en buscar poder de manera engañosa sobre varias partes de la sociedad: cómo influir a políticos con información incompleta o falsa —por cierto, una compañera diputada me acaba de comentar que ayer hubo una clase magistral sobre esto en *La noche en 24 horas* de Televisión Española; habrá que verlo—; financiar la desinformación en los medios o investigadores y evadir la responsabilidad usando las leyes, o sea, usándonos a nosotros. Al igual que el dinero se traduce en poder, muchas capacidades de la inteligencia artificial, como el engaño, también se traducen en poder. Como ha dicho el señor Asarta, lo vivimos directamente anteayer mismo, las consecuencias del uso de la inteligencia artificial sobre la población civil, en este caso por el ejército de Israel en el genocidio de Gaza, evidencian la urgente necesidad de su regulación sobre la base de principios éticos.

Para acabar, creemos que es necesario protegerse, sobre todo, de las *deepfakes,* que implican una combinación de precauciones tecnológicas, educación y ámbitos de verificación. Ahí a SUMAR siempre la encontrarán.

Gracias.

La señora **PRESIDENTA:** Antes de la intervención del Grupo Parlamentario Izquierdas por la Independencia, Esquerra Republicana, debo aclarar, señor Gaseni, que ustedes han pedido la traducción, pero, al haberlo hecho fuera de plazo, según el acuerdo del Congreso de enero de este año, le tengo que pedir que, si quiere hacer su intervención en catalán, haga usted mismo la traducción al castellano; o, alternativamente, según —vuelvo a citar— el acuerdo de la Cámara de enero de este año, usted nos tendría que presentar por escrito su intervención en castellano a lo largo de la sesión.

Dicho esto, señor Gaseni, le doy la palabra, repito, por el Grupo Parlamentario Republicano Izquierdas por la Independencia, Esquerra Republicana.

El señor **GASENI BLANCH:** Bon dia.

Presidenta, no sé, creíamos que lo habíamos hecho en tiempo y forma, pero lo que sí haremos, con permiso de la Mesa, es hacer lo que teníamos preparado en catalán, poco a poco, y ya les pasaremos la traducción de lo que tenemos preparado. Creo que igual que yo entiendo perfectamente a sus señorías, ustedes van a poder entenderme a mí con una explicación pausada y que sea totalmente entendible. Ya le digo que le enviaremos esta traducción.

La señora **PRESIDENTA:** Disculpe, pero le recuerdo el acuerdo de la Cámara, porque usted está hablando de enviarlo. Tendría que entregarlo a lo largo de la sesión por escrito.

El señor **GASENI BLANCH:** Sí, pues a lo largo de la sesión, me veo capaz de poder hacer la traducción.

La señora **PRESIDENTA:** O traducirlo usted, le podemos dar un poco más de tiempo.

El señor **GASENI BLANCH:** Bueno, no hace falta, que tampoco quiero molestar a sus señorías, que seguramente tendrán otras comisiones a lo largo de la mañana. Ya verán que es muy fácil. **(Continúa su intervención en catalán, cuya traducción se incluye a continuación según el texto facilitado por el señor diputado a la Comisión).**[1]

Señorías

Vivimos en un mundo donde cada día que pasa las tecnologías avanzan más rápido del que las podemos entender y del que las podemos regular. La inteligencia artificial, la computación cuántica, todo esto va no una, sino centenares de pasas por delante. Es la realidad que ya nos rodea, aunque no la vemos. Y si no somos capaces de entender los riesgos que esto comporta, estaremos perdiendo una

[1] En aplicación del punto Tercero.7 del Acuerdo de la Mesa del Congreso de los Diputados relativo al régimen lingüístico de los debates en los órganos parlamentarios, conforme al cual la veracidad de la traducción es responsabilidad del diputado.

cve: DSCG-15-CM-43

oportunidad de oro para proteger aquello que más nos importa: nuestros derechos, nuestra libertad y nuestro bienestar presente y futuro.

De entrada, parece un tema técnico, de estos que hacen bostezar además de uno y que tenemos que dejar en manos de los técnicos, de los «expertos». Pero es mucho más que esto. Es profundamente político y lo nos remangamos para intentar controlar el torrente de cambios que se acercan o nos pasará por sobre como un tsunami.

Y aquí viene el quid de la cuestión. Las nuevas tecnologías son una maravilla, pero también son una herramienta de poder brutal. Quién controla la tecnología controla la información, y quien controla la información, controla el mundo. Sí, la realidad es que un puñado de grandes corporaciones multinacionales, como Google, Amazon o Facebook, tienen más poder que muchos estados. Y mientras hablamos de ciberseguridad, el que realmente tenemos que hacer es asegurarnos que estas empresas no nos están utilizando cómo simples mercancías.

Cataluña, como nación, tiene que tener voz propia en este debate. No podemos depender de unas pocas empresas que deciden qué se hace con nuestros datos, como se usan y qué riesgos corremos. Desde Cataluña exigimos soberanía digital, no volamos ni podemos acontecer simples espectadores de un futuro que nos pasa por sobre.

Además, hablamos de nuestros derechos. La IA se usa ya a muchos lugares del mundo para vigilarnos, para clasificarnos, para controlarnos. Y si no ponemos límites, estamos abriendo la puerta en un mundo donde nuestras vidas estarán bajo la lupa de algoritmos que deciden qué podemos hacer, qué podemos decir e incluso qué podemos pensar.

Por lo tanto, esta ponencia nos gustaría que no solo abordara la seguridad como un tema técnico, sino como una cuestión de derechos humanos. Tenemos que garantizar que la IA no se convierta en una herramienta de represión o discriminación. Y, francamente, no tenemos que ir mucho lejos para ver como se pueden utilizar estas tecnologías para la vigilancia política. El caso Pegasus, el espionaje a líderes independentistas, es la prueba de como las herramientas digitales pueden ser utilizadas para silenciar voces críticas y vulnerar derechos fundamentales. Esto es el que queremos evitar, no solo por Cataluña, sino para todo el mundo.

Con la computación cuántica, la ciberseguridad tal como la conocemos hoy puede quedar obsoleta en un santiamén.

Porque aquí no se trata solo de seguridad, se trata de soberanía. No podemos seguir delegando en otros países o corporaciones la protección de nuestra información y nuestras infraestructuras. Cataluña tiene que tener la capacidad de gestionar su propio futuro digital, con control propio sobre sus datos y sus sistemas.

Pero esto solo lo conseguiremos si somos capaces de entender que la seguridad digital va más allá de los técnicos y los especialistas. Va de política, va de derechos, va de nuestra capacidad para construir una sociedad más justa y libro en un mundo cada vez más interconexionado.

Moltes gràcies.

La señora **PRESIDENTA:** Señor Gaseni, le vuelvo a recordar la necesidad de presentar la traducción. ¿Nos la va a presentar por escrito, por lo tanto, a lo largo de la sesión?

El señor **GASENI BLANCH:** Sí, sí, en breves minutos.

La señora **PRESIDENTA:** De acuerdo, muchas gracias.

A continuación, por los grupos parlamentarios Euskal Herria Bildu e Izquierdas por la Independencia, Euskal Herria Bildu, tiene la palabra don Jon Iñarritu.

El señor **IÑARRITU GARCÍA:** Egun on, presidente andrea. Buenos días, señorías.

Está ya prácticamente todo dicho, pues soy el último que voy a intervenir. Es cierto que todo lo que representa la inteligencia artificial y el ciberespacio es un mundo de oportunidades. Dense cuenta de que, por ejemplo, la intervención que hace instantes ha hecho el compañero de Esquerra Republicana se podría traducir gracias a la inteligencia artificial en escasos segundos y, si alguien ha tenido dificultad para entender lo que ha dicho, no haría falta que la entregase. Pero es cierto que, como suele ocurrir en esta vida, todo lo que representa oportunidades también representa en muchas ocasiones riesgos. Los riesgos y las amenazas que suponen la inteligencia artificial y el ciberespacio están ahí y son numerosos —se han enumerado en el documento presentado— y todo lo que nos lleve a intentar analizar, a entender, incluso

cve: DSCG-15-CM-43

a proponer mejoras a las instituciones para dotar de mayor seguridad tanto a estas como a las empresas y a la ciudadanía, es positivo.

Decía el proponente que esto nos va a permitir analizar en profundidad. Bueno, yo no sé si vamos a poder hacerlo en profundidad, pero sí creo que es un ejercicio positivo. No es la primera vez que está Comisión —en otras legislaturas ya lo ha hecho— va a analizar algunas de esas amenazas que están ahí —ya se han presentado documentos y recomendaciones—, y que lo vaya a hacer en esta legislatura es también positivo. También es cierto que, en España, en el Estado, esto no es *ex novo,* ya existen agencias, ya existe el Centro Criptológico, el INCIBE, el OSI, y los cuerpos policiales están dotados también de brigadas y de grupos que analizan los ciberdelitos. Pero ya digo que todo lo que vaya en la vía de intentar entender, analizar y recomendar, sobre la base de lo que nos puedan decir los expertos y las expertas, es positivo.

Hemos sido testigos, incluso en este Congreso, de cómo en ocasiones la web del Congreso no funcionaba, presuntamente debido a ciberataques. De igual forma —lo comentaba el compañero de Esquerra—, en España en estos años se ha producido el mayor ataque conocido en territorio de la Unión Europea a teléfonos móviles de cargos públicos, abogados, representantes asociativos… Este caso, curiosamente, quedó prácticamente en su totalidad irresuelto, sin saber quién estaba detrás de ese ataque. Yo creo que todos los ejercicios que nos permitan intentar descubrir o intentar proponer medidas para que no se produzcan hechos así van en la buena línea.

Como se presupone por la intervención que he realizado, apoyaremos la creación de la ponencia.

Muchas gracias. Eskerrik asko.

La señora **PRESIDENTA:** Dado que no veo a ningún representante del Grupo Parlamentario Vasco (EAJ-PNV), damos por concluido el debate.

Votaremos en tres minutos. **(Pausa).**

Antes de proceder a la votación, quería trasladarles que esa traducción que hemos pedido para cumplir con el acuerdo de la Cámara ya ha sido enviada telemáticamente por el señor Gaseni al letrado, y figurará en el *Diario de Sesiones,* si no hay ningún problema o desacuerdo por parte del resto de los grupos. **(Denegaciones).**

Pasamos, a continuación, a la votación. Se votará la propuesta de creación de ponencia en los términos en que ha sido distribuida a lo largo de la sesión, ya que, como verán, hay unas correcciones técnicas, de las que hablamos ya en la reunión de Mesa y portavoces.

Pasamos a la votación. **(Pausa).**

Efectuada la votación, dio el siguiente resultado: votos a favor, 36.

La señora **PRESIDENTA:** Queda aprobada la creación de la ponencia. **(Aplausos.—Varios señores diputados: ¡Muy bien!).**

Al no haber más asuntos que tratar, se levanta la sesión.

Eran las nueve y cuarenta y cinco minutos de la mañana.

cve: DSCG-15-CM-43