BOLETÍN OFICIAL
DE LAS CORTES GENERALES

SECCIÓN CORTES GENERALES

XIV LEGISLATURA

Serie A:
ACTIVIDADES PARLAMENTARIAS **9 de febrero de 2021** **Núm. 105** **Pág. 1**

ÍNDICE

cve: BOCG-14-CG-A-105

CONTROL DE LA ACCIÓN DEL GOBIERNO

PROPOSICIONES NO DE LEY/MOCIONES

Comisión Mixta de Seguridad Nacional

161/001940 (CD)
663/000082 (S)

La Mesa del Congreso de los Diputados, en su reunión del día de hoy, ha adoptado el acuerdo que se indica respecto al asunto de referencia.

(161) Proposición no de Ley en Comisión.

Autor: Grupo Parlamentario VOX.

Proposición no de Ley por la que se insta al Gobierno a llevar a cabo todas las acciones pertinentes para impedir la participación de proveedores tecnológicos chinos en la red 5G de España, dado el riesgo que lo anterior supone para la Seguridad Nacional española.

Acuerdo:

Considerando que se solicita el debate de la iniciativa en Comisión, y entendiendo que es la Comisión Mixta la que insta al Gobierno a la adopción de las medidas correspondientes, admitirla a trámite como Proposición no de Ley, conforme al artículo 194 del Reglamento, y disponer su conocimiento por la Comisión Mixta de Seguridad Nacional. Asimismo, dar traslado del acuerdo al Gobierno, al Senado, al Grupo proponente y publicar en el Boletín Oficial de las Cortes Generales.

En ejecución de dicho acuerdo, se ordena la publicación.

Palacio del Congreso de los Diputados, 2 de febrero de 2021.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

A la Mesa del Congreso de los Diputados

D.ª Macarena Olona Choclán, D. Víctor González Coello de Portugal y D. Julio Utrilla Cano, en su condición de Portavoz Adjunta y Diputados del Grupo Parlamentario VOX (GPVOX), al amparo de lo establecido en el artículo 193 y siguientes del vigente Reglamento del Congreso de los Diputados, presentan la siguiente Proposición no de Ley relativa a instar al Gobierno a llevar a cabo todas las acciones pertinentes para impedir la participación de proveedores tecnológicos chinos en la red 5G de España, dado el riesgo que lo anterior supone para la Seguridad Nacional española, para su discusión en la Comisión Mixta de Seguridad Nacional.

Exposición de motivos

Primero. El auge de China y su particular disputa con los Estados Unidos de América por la hegemonía mundial está provocando lo que los expertos conocen como «Trampa de Tucídides»[1]. Esta hipótesis señala que la guerra es inevitable cuando una potencia emerge y existe otra dominante. Concretamente, el caso que relató el historiador griego Tucídides, en su narración de la Guerra del Peloponeso, fue el de Atenas y Esparta. En dicho conflicto bélico, el autor señaló que la guerra era inevitable dado el ascenso de Atenas y el miedo que eso inspiró en Esparta[2].

[1] «Qué es la trampa de Tucídides por la que se teme que estalle una guerra entre EE.UU. y China», BBC Mundo. 20.08.2017. Disponible [en línea]: https: / / www.bbc.com/ mundo/noticias-40974871

[2] Para profundizar más en esta materia, véase: ALLISON, Graham, Destined for War: Can America and China Escape Thucydides' s Trap? Houghton Mifflin Harcourt, New York, 2017. En este libro, el politólogo y asesor de seguridad nacional Graham Allison, apunta que en los últimos 500 años se han producido 16 casos en los que el ascenso de una gran nación trastocó la posición de otra nación dominante. Doce de ellos terminaron provocando una guerra. Esto es, en un 75 % de los casos.

cve: BOCG-14-CG-A-105

Con el objetivo de arrebatar a Estados Unidos el liderazgo global, China no ha dudado en utilizar todas las herramientas a su disposición, como es el caso del ciberespionaje. Así, a la vista de la superioridad militar que todavía detenta Estados Unidos, el país asiático emplea estrategias de «zona gris». En este sentido, en palabras del profesor Javier Jordán, «la zona gris es un espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política, del enfrentamiento armado directo y continuado. El conflicto en la zona gris gira en torno a una incompatibilidad relevante para al menos uno de los actores. Las estrategias utilizadas son multidimensionales, de implementación gradual u con objetivos a largo plazo» [3].

De esta forma, entre las líneas de acción estratégicas empleadas en la zona gris, se encuentran los « ciberataques contra entidades públicas y privadas» [4]. Concretamente, Jordán destaca lo siguiente:

«[...] además de amedrentar y generar confusión en el proceso de toma de decisiones políticas, airean la vulnerabilidad del adversario (Baques, 2017: 22; Wirtz, 2017: 108). Pueden ser ataques de diversa consideración: desde denegaciones temporales de servicio en sitios zveb institucionales a acciones de mayor calado como los famosos ciberataques sufridos por Estonia en 2007 (Kramer y Speranza, 2017: 8-9). También pueden entrar en esta categoría —siempre que se efectúen en el marco de un conflicto en la zona gris— las acciones de ciberespionaje económico realizadas por las agencias de un Gobierno para abaratar los costes de investigación y desarrollo de su país, apropiándose de los avances obtenidos por las empresas de otros, una acusación que frecuentemente recae sobre las agencias de inteligencia chinas (Frier, 2016: 38). La dificultad de confirmar la autoría de este tipo de episodios se ajusta a unas estrategias que como ya se ha señalado se caracterizan por su ambigüedad»[5].

No obstante, este señalamiento hacia China no es baladí. Es de sobra conocido que el orden internacional liberal que ha regido desde la conclusión de la Guerra Fría se encuentra en un momento delicado, tanto que la crisis provocada por el COVID-19 puede ser la causa definitiva de su derrumbe. Y es que, durante arios, los principales poderes del Viejo Continente —Alemania, Francia y Reino Unido—, se han dedicado a incentivar las relaciones comerciales con China, con la falsa esperanza de que éstas favoreciesen el inicio de un proceso democratizador en el país asiático.

Estas tesis, defendidas por autores de gran prestigio como Ronald Inglehart o Christian Welzel, son cuestionadas por la nueva realidad que emerge ya bien entrado el siglo XXI. Con unas prácticas propias de un régimen mercantilista, el Partido Comunista Chino se ha servido del sistema capitalista y de la defensa a ultranza de éste por parte de las potencias occidentales, para mantener un crecimiento exponencial de su economía durante tres décadas. Gracias a esta bonanza, el régimen autoritario chino ha conseguido aumentar la renta disponible de gran parte de su población. Como contrapartida, el politburó no ha abierto la mano en cuanto a reformas políticas que favorezcan las libertades individuales y los derechos políticos y sociales de sus ciudadanos. Más bien todo lo contrario.

Recordemos que el pasado 28 de mayo, el Parlamento orgánico del régimen chino aprobaba imponer a Hong Kong una controvertida Ley de Seguridad Nacional que desató una fuerte oposición en la excolonia británica y entre la comunidad internacional. La aprobación de ésta se desarrolló sin ningún debate, por 2.878 votos a favor, uno en contra y seis abstenciones.

El motivo de la fuerte oposición expresada por la comunidad internacional es que se considera una violación del principio de «un país, dos sistemas» que otorga a la ciudad autónoma más libertades que al resto de China y que, en teoría, está vigente hasta el año 2047, en virtud del acuerdo de devolución suscrito con el Reino Unido.

La ley establece en Hong Kong oficinas de la seguridad pública china, algo que horroriza a los habitantes de la ciudad por su fama de intimidar y hacer «desaparecer» a los disidentes en el continente, donde la Policía puede retener legalmente a los sospechosos hasta seis meses para interrogarlos sin pasar por un tribunal, señalan diversas fuentes de información pública.

Por ello, el pasado 2 de junio, los presidentes de las comisiones de Asuntos Exteriores de Australia (David Fawcett), Canadá (Michael Levitt), Nueva Zelanda (Simon O'Connor) y Reino Unido (Tom Tugendhat), dirigieron una carta al secretario general de la ONU, Antonio Guterres, solicitando que, en

[3] JORDAN, Javier: «El conflicto internacional en la zona g-ris: una propuesta teórica desde la perspectiva del realismo ofensivo», Revista Española de Ciencia Política, n°48, noviembre 2018, pp.129-151. Disponible [en línea]: https:/ /www.ugr.es/---jjordan/Conflicto-zona-gris.pdf

[4] Op. Cit. P. 139.

[5] Op. Cit.

cve: BOCG-14-CG-A-105

colaboración con el Consejo de Derechos Humanos de las Naciones Unidas, se procediera a otorgar un mandato para el envío de un convoy especial a Hong Kong.

Así, la gravedad de la amenaza que supone el Partido Comunista Chino —y las empresas chinas que controla— para Occidente, quedó reflejado el pasado 23 de julio de 2020, en un discurso[6] del secretario de Estado americano, Mike Pompeo. Dicho discurso se enmarca en una serie de conferencias impartidas por el Consejero de Seguridad Nacional, Robert O'Brien, el director del FBI, Chris Wray y el Fiscal General William Barr. El alto perfil de los ponentes previos al secretario es la mejor prueba de la prioridad que la Administración estadounidense ha dado a la cuestión.

En su discurso, el secretario Pompeo destacó los enormes desequilibrios existentes en la relación entre Estados Unidos y China, fruto de la dejadez de las anteriores Administraciones. Esta atrofia geopolítica estadounidense ha favorecido el auge de China hasta convertirse en la principal amenaza para «el futuro de las democracias libres en todo el mundo».

Tras medio siglo de seguimiento de la falacia kantiana de la paz perpetua, del «viejo paradigma del compromiso ciego», que postula que China se democratizaría mediante la cooperación y el comercio, Estados Unidos ha decidido cambiar de estrategia. En palabras del secretario de Estado, «no debemos continuarla [la estrategia del compromiso ciego] y no debemos volver a ella» . Y finalizó, «... la única forma de cambiar verdaderamente a la China comunista es actuar no sobre la base de lo que dicen los líderes chinos, sino cómo se comportan... Nosotros, las naciones del mundo amantes de la libertad, debemos inducir a China a cambiar, tal como quería el presidente Nixon. Debemos inducir a China a cambiar de manera más creativa y asertiva, porque las acciones de Beijing amenazan a nuestro pueblo y nuestra prosperidad» . Y para ello, el resto de las naciones libres tienen «que llegar a su propia comprensión de cómo proteger su propia soberanía, cómo proteger su propia prosperidad económica y cómo proteger sus ideales de los tentáculos del Partido Comunista Chino».

Las acciones descritas han puesto de relieve la agresividad con que actúa China en el tablero mundial, así como su verdadero objetivo: arrebatar la hegemonía mundial al máximo representante de los valores liberales occidentales, los Estados Unidos de América.

Segundo. Esta asertividad se plasma en las actuaciones que el régimen comunista está llevando a cabo en el campo de las tecnologías de la información. A diferencia de lo que ocurrió con el despliegue de las redes 3G y 4G, China adoptó como plan de país ser pionero en el desarrollo de la tecnología 5G, como una rama fundamental en su estrategia de información, tanto ad intra como ad extra. Y ello a fin de controlar estrictamente el flujo de información dentro del país mientras se aprovecha de la información para influir en las sociedades extranjeras.

Resulta evidente que la implantación de la tecnología 5G a nivel global es una oportunidad inmejorable para que cualquier potencia emergente intente ampliar su poder y capacidad económica a costa de la información y conocimiento de otros países. Por tanto, resulta igualmente evidente que cualquier país que quiera mantener su independencia, soberanía, influencia, seguridad nacional, e incluso la supervivencia de su propia industria, deber proteger al máximo sus telecomunicaciones y, por ende, su red de 5G.

En particular, esta tecnología está llamada a provocar un impacto disruptivo en la sociedad digital y a revolucionar nuestra manera de entender el intercambio de información en el siglo XXI, con las consecuentes implicaciones geopolíticas. El 5G traerá una alta velocidad de transferencia, una mayor capacidad de conexión y una baja latencia en las comunicaciones. En consecuencia, permitirá que se pongan en marcha y perfeccionen productos y servicios en los que se requiera una alta velocidad (aplicaciones multimedia o de realidad aumentada), así como el despegue definitivo del internet de las cosas (Internet of Things -IoT) por la posibilidad de tener simultáneamente conectado un volumen ingente de dispositivos.

Asimismo, posibilitará definitivamente las aplicaciones que requieran respuestas en tiempo real (industria 4.0, cirugía remota asistida, videojuegos), además de la expansión de servicios basados en decisiones automatizadas, muchas veces usando inteligencia artificial (smart cities). En la telefonía móvil, el 5G supone adicionalmente un cambio sustancial con relación a las generaciones anteriores: por primera vez dejará de utilizarse hardware específico de telefonía para dar paso a equipos «de propósito general», idénticos a los que pueden encontrarse en un centro de procesamiento de datos TIC. Ello representa ventajas en materia de costes y de flexibilidad de implementación y hace que la infraestructura sea interoperable y accesible por una multiplicidad de equipos en Internet.

[6] https://www.state.pv/communist-china-and-the-free-worlds-future/

cve: BOCG-14-CG-A-105

Así, tres son las características que permiten calificar al 5G como una tecnología disruptiva y como cambio de paradigma en la concepción de las redes de comunicaciones móviles:

— Virtualización: la utilización de las tecnologías de virtualización es lo que podría suponer una mayor revolución y, consecuentemente, un más grande impacto en la privacidad. En este ámbito se incluyen nuevos conceptos como:

1. Software Defined Networking (SDN), que facilitará a los operadores realizar cambios en la red de forma rápida y, en algunas circunstancias, también de forma automática, adaptándose a las necesidades de demanda en la red.
2. Network Function Vírtualization (NFV), que supone crear, desplegar y gestionar servicios de red virtualizando todas y cada una de las funciones que proporciona la propia red.
3. Network Slicing (NS), que implica mejorar y adaptar el soporte a diferentes tipos de tráfico en las redes 5G, subdividiendo las redes core en un conjunto de slices o redes core virtuales.

— Edge computing: el uso de hardware de propósito general para contener servicios virtualizados del operador o de otros proveedores de servicios permitirá implementar los denominados MEC (Multi-Access Edge Computing), desplazando el centro de gravedad del tratamiento de datos desde los servidores hacia ubicaciones más cercanas al dispositivo terminal del usuario, cuando sea necesario. Esto es, podrá existir un flujo de información o servicios entre diferentes ubicaciones acordadas por operadores de la red y gestores de servicios, en puntos cercanos al usuario final y dentro de la red de telefonía móvil de un operador de telecomunicaciones, en principio sin estar en Internet. Por tanto, ello permitirá una reducción en la latencia de las comunicaciones tal que permitirá contar con capacidades próximas al tiempo real.

— Localización: el 5G necesitará una red de acceso mucho más compacta, con muchos puntos de acceso y menor distancia entre ellos, lo que proporcionará al operador y a otros agentes vinculados a la explotación de los datos de la red la capacidad de localizar el terminal de usuario con una precisión mucho mayor de la que tiene en la actualidad. Se alcanzarán resoluciones de localización inferiores a un metro y, al contrario que las generaciones previas a 5G, incluyendo posicionamiento en tres dimensiones.

Por tanto, con estas capacidades y atributos en su poder, el régimen comunista chino gozaría de un poder omnímodo sobre las comunicaciones y, por tanto, sobre los países en los que sus empresas tecnológicas operen y controlen la red 5G.

En adición a lo anterior, hay que tener en cuenta que el Partido Comunista de China tiene a gala el uso del «discourse power»[7]: la creación y difusión de narrativas y relatos que sirven a los intereses del Estado chino y la eliminación de aquellos que amenazan su integridad. Para ello, se busca la consecución de un «Internet armonioso» en el que se persigue el disenso, se ponen en marcha instituciones como la Administración del Ciberespacio de China (CAC), se compran medios de comunicación en países africanos y se enseña a los diplomáticos chinos a manejar redes sociales occidentales (prohibidas en su propio país) y a aumentar el impacto mediático de sus declaraciones. Y, como brazo ejecutor de esta política, se encuentra la empresa Huawei.

Tercero. Huawei, fundada por Ren Zhengfei, ingeniero y exsoldado de la rama militar del Partido Comunista Chino, así como actual miembro destacado de este partido, es la primera auténtica multinacional global china, la cual da trabajo a 194.000 personas (de ellas, 1.200 en España) y consiguió el pasado ario un beneficio de diez mil millones de euros. Además, es el mayor proveedor tecnológico del mundo, con un 28 % del mercado global.

Además, Huawei controla casi medio centenar de contratos comerciales para la instalación de las infraestructuras de 5G (más de la mitad en Europa), y ha suscrito acuerdos de colaboración con diversos operadores europeos. Su principal ventaja en el nicho de mercado del 5G es que puede hacer equipos para toda la cadena de distribución: produce los chips de los smartphones, routers, core y demás elementos de la infraestructura de red. Asimismo, este proveedor es el que más contribuciones técnicas ha presentado a los estándares del 5G (más de 10.000, frente a las 8.400 de Ericsson y las 5.800 de Nokia), y también el que tiene más patentes registradas (1550, por 1427 de Nokia).

[7] FAWCETT, Alicia: «Chinese Discourse Power. China's use of Information Manipulation in Regional and Global Competition», Atlantic Council, October 2020. Disponible [en línea]:
https://www.atlanticcouncilorg/wp-content/uploads/2020/10/Chinese-Discourse-Power.pdf

cve: BOCG-14-CG-A-105

No obstante lo anterior, sobre esta compañía pesan numerosas acusaciones de espionaje generalizado a Gobiernos y a empresas de países occidentales, además de ser el brazo de vigilancia del Partido Comunista y del Gobierno chino —y suministrarle información confidencial—, así como de colaborar en la represión de más de un millón de musulmanes pertenecientes a la minoría étnica uigur en Xinjiang. Así, a pesar de que Huawei ha desmentido estas últimas afirmaciones, tras meses de investigaciones y pruebas, las informaciones se han confirmado. [8]

Así pues, diversas instancias internacionales han alertado en este sentido de los riesgos para la privacidad y los derechos humanos en los que podrían estar incurriendo las acciones de Huawei. Por su parte, la revista Forbes publicó en 2019 un artículo en el que aseguraba que la avanzada tecnología de Huawei estaba siendo empleada para la vigilancia de los uigures en Xinjiang y para el monitoreo de sus móviles. Ese mismo año, el Wall Street Journal informó de que el Gobierno chino habría concedido 75.000 millones de dólares a esta empresa a través de distintos medios de asistencia financiera[9]

Adicionalmente, el Instituto de Política Estratégica de Australia (ASPI) publicó un informe señalando que «el trabajo de Huawei —y otras compañías tecnológicas chinas— en Xinjiang es extenso e incluye trabajar directamente con las oficinas de seguridad pública del gobierno chino en la región»[10]

Por si esto no fuera suficiente, el National Cyber Security Centre del Reino Unido (NCSC), el cual había señalado en marzo de 2019 que no había encontrado evidencia de actividad maliciosa del Estado chino en Huawei pero que sí había identificado algunos defectos graves en la ingeniería de software y en la competencia de seguridad cibernética de la compañía, ha anunciado recientemente que «ha cambiado significativamente su evaluación de seguridad» sobre la presencia de Huawei en la red 5G de Reino Unido y recomendó el veto a dicho proveedor. En este sentido, el Gobierno británico y sus aliados han responsabilizado a «elementos del gobierno chino de realizar una gran campaña cibernética global contra propiedad intelectual e información comercial sensible en Europa, Asia y Estados Unidos»[11]

Así pues, el por entonces ministro de Asuntos Exteriores británico, Jeremy Hunt, señaló lo siguiente:

«Esta campaña es una de las intrusiones cibernéticas más significativas y generalizadas contra el Reino Unido y sus aliados descubiertos hasta la fecha, apuntando a secretos comerciales y economías de todo el mundo. Estas actividades deben cesar. Van en contra de los compromisos contraídos con el Reino Unido en 2015, y, como parte del G20, relativas a no llevar a cabo o apoyar el robo cibernético de la propiedad intelectual o secretos comerciales. Nuestro mensaje a los gobiernos preparados para permitir estas actividades es claro: junto con nuestros aliados, expondremos sus acciones y tomaremos otras medidas necesarias para asegurar que se respete el estado de derecho»[12].

Por su parte, el Departamento de Comercio de los Estados Unidos publicó una lista negra con las empresas consideradas como una amenaza para la seguridad nacional, entre las que se encuentra Huawei.[13] En adición, la Comisión Europea ya ha alertado de que «las amenazas a la ciberseguridad (incluido el riesgo de intromisión de agentes de Estados no miembros de la UE o que cuenten con su respaldo) son un reto en constante evolución y cuya importancia aumenta al ritmo de la creciente dependencia de la tecnología y los datos»[14]

Asimismo, la Comisión Europea, la presidencia finlandesa del Consejo de la Unión Europea y la Agencia Europea de Ciberseguridad (ENISA) publicaron en octubre de 2019 un informe sobre la evaluación coordinada de riesgos realizada por la UE acerca de la seguridad de las redes 5G, en el cual alertaron de que esta tecnología «facilitará un mayor número de vías de ataque que podrían ser explotadas por agentes de riesgo y aumentará la gravedad potencial del efecto de tales ataques. Entre los distintos

[8] S.I: «Huawei retira su plan de patente para identificar uigures», ABC, 15.01.2020. Disponible [en línea]: https: / /www.abc.es/ internacional/abci-huawei-retira-plan-patente-para-identificaruigures-202101150108 noticia.html

[9] Chuin-Wei Yap: «State Support helped fuel Huawei's global rise», The Wall Street Journal, 25.12.2019. Disponible [en línea]: https: / /www.wsj.com/articles/state-support-helped-fuelhuaweis-global-rise-11577280736

[10] «Huawei and Australia's 5G Network: Views from ASPI», Australian Strategic Policy Institute, Report No. 8/2018. Disponible [en línea]: https:/ /s3-ap-southeast-2.amazonaws.com/adaspi/2018-10/Huawei%20and%20Australias%205G%20Network.pdf?wk2qurC5OGPs1DZmePkkYm bK w8Rn5Yj

[11] Press Release UK GOV: «UK and allies reveal global scale of Chinese cyber campaign». 20.12.2018. Disponible [en línea]: https: / / www.gov.uk/ government/ news/ uk-and-alliesreveal-global-scale-of-chinese-cyber-campaign

[12] Op.cit.

[13] «Bureau of Industry and Security, U.S. Department of Commerce. Disponible [en línea]: haps: / / www.bis.doc. goy/ index. php / regulations/ export-administration-reg-ulations-ear

[14] «Despliegue seguro de la 5G en la UE- Aplicación de la caja de herramientas de la UE», Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Comisión Europea, p.14. 29.01.2020. Disponible [en línea]: https:/ /eur-lex.europa.eu/legal-content/ES/TXT/PDF/ ?uri=CELEX:52020DC0050&from=FR

cve: BOCG-14-CG-A-105

agentes potenciales, los Estados no pertenecientes a la UE o aquellos respaldados por Estados son los más peligrosos y los que más probabilidades tienen de atacar las redes 5G».

Sin perjuicio de lo anterior, Estados Unidos y el Reino Unido no se han quedado solos en el veto a Huawei. Países como Australia, Nueva Zelanda y Japón también han bloqueado el acceso de la empresa china a su red de 5G. Incluso Suecia, país conocido por su equidistancia en las rivalidades por el poder, ha bloqueado la entrada tanto a Huawei como a ZTE en su red 5G.[15] Además, se están llevando a cabo investigaciones sobre la falta de seguridad y, por tanto, la interferencia del gobierno chino sobre las comunicaciones (ciberespionaje,) en las redes gestionadas por Huawei en Francia y Alemania.

Cuarto. En lo que a España se refiere, cabe destacar que el pasado 15 de julio, la Ministra de Asuntos Exteriores, Unión Europea y Cooperación, la señora Arancha González Laya, mantuvo una reunión con el secretario de Estado estadounidense, Mike Pompeo, en la que según señaló la propia Ministra, se trataron temas como «la recuperación económica post COVID-19, la fiscalidad de actividades digitales, de 5G, de la agenda común entre España y EE. UU. en la OTAN y la movilidad internacional para profesionales y estudiantes» .

A raíz de lo anterior, el 17 de julio de 2020, el Grupo Parlamentario VOX se interesó mediante pregunta con respuesta escrita —con número de registro 46421— por los temas tratados en la citada reunión y, en particular, sobre la posibilidad de limitar la entrada de proveedores chinos en la red 5G de España. Por su parte, el Gobierno, en su respuesta escrita fechada el 22 de septiembre de 2020 —con número de entrada 56657—, señaló lo siguiente:

«El Gobierno considera que una rápida y completa implantación en todo el territorio nacional de la tecnología de telefonía móvil 5G es una prioridad para el desarrollo de las comunicaciones y la modernización de la economía en nuestro país. El Gobierno facilitará, por ende, el marco general y las condiciones objetivas para un acceso de las administraciones públicas, los agentes económicos, las empresas y los particulares a una tecnología digital 5G abierta, segura y asequible.

Para ello, garantizará que haya una diversificación de proveedores confiables, así como una seguridad en el suministro del servicio y la privacidad de las comunicaciones. Todo ello en cumplimiento de las Recomendaciones y de la «caja de herramientas» acordadas por la Comisión Europea para prevenir y mitigar posibles vulnerabilidades derivadas de la implantación de las tecnologías 5G.

España milita a favor de una autonomía estratégica y una soberanía tecnológica y digital de la Unión Europea, que permita a sus Estados miembros, incluido nuestro país, contar con nuestros propios operadores y tecnologías, también en la decisiva tecnología 5G. Mientras tanto, se apuesta por un acceso al mercado abierto, libre y justo, sin plantearnos fijar cuotas de mercado a determinadas compañías.

Por otra parte, cabe indicar que el pasado jueves 23 de julio, el Presidente del Gobierno presentó la nueva Agenda Digital que llevará el nombre de España Digital 2025. Esta Agenda incluye cerca de 50 medidas agrupadas en diez ejes estratégicos.

Uno de estos ejes es el de seguir liderando el despliegue de la tecnología 5G en Europa e incentivar su contribución al aumento de la productividad económica, al progreso social y a la vertebración territorial. En ella se fija como objetivo que en 2025 el 100 % del espectro radioeléctrico esté preparado para el 5G.

[15] Mukherjee, Supanta y Soderpalm, Helena: «Sweden bans Huawei, ZTE from upcoming 5G networks», Reuters. 20.10.2020. Disponible [en línea]: https:/ /www.reuters.com/ article/uk-sweden-huawei-idUKKBN2750VL

cve: BOCG-14-CG-A-105

En la consulta pública para recabar aportaciones en relación con la elaboración de normas sobre la seguridad de las redes y servicios de comunicaciones móviles de quinta generación o 5G, ya se recogía a la cadena de suministro como clave para mantener la seguridad de la red. Tal y como figuraba en la Recomendación (UE) 2019/534 donde se alude a este tipo de amenaza como un riesgo no tecnológico u «otros factores» de riesgo.»

Por tanto, a pesar de todo lo anteriormente expuesto, y a la luz de la respuesta emitida por el Gobierno, mientras nuestros principales socios y aliados vetan o al menos se encuentran actualmente investigando tanto a Huawei como al resto de proveedores tecnológicos chinos de red 5G, el Gobierno español presume de seguir colaborando con ellos.

Quinto. Resulta verdaderamente difícil la consecución del postulado del Gobierno sobre «seguir liderando el despliegue de la tecnología 5G en Europa», así como el objetivo de «que en 2025 el 100 % del espectro radioeléctrico esté preparado para el 5G», sobre todo teniendo en cuenta que nuestro país todavía no tiene un marco normativo propio que establezca y asegure los criterios, obligaciones y las condiciones de seguridad mínimas que deban aportar los proveedores que estén interesados en operar en nuestra red de 5G. Por ello, parece inconcebible que el presidente del Gobierno realice declaraciones como las siguientes:

«Antes de que termine este año, el 75 % del territorio español va a tener acceso a la tecnología 5G. Y lo estamos haciendo con distintas empresas también extranjeras».

No obstante, pese a no existir un marco normativo propio que, como se ha comentado anteriormente, establezca y asegure los criterios, obligaciones y las condiciones de seguridad mínimas que deban aportar los proveedores que estén interesados en operar en nuestra red de 5G, sí se puede abordar este tema desde el ámbito de la Seguridad Nacional. En concreto, la Ley de 36/2015, de 28 de septiembre, de Seguridad Nacional, contempla en su artículo 10 los ámbitos de especial interés de la Seguridad Nacional, a saber, los siguientes:

«Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente».

En el siguiente plano normativo, la Estrategia de Seguridad Nacional de 2017 destaca el espionaje como una de las principales amenazas a las que se enfrenta nuestro país. En concreto, dicha estrategia señala lo siguiente:

«El espionaje es una amenaza de primer orden para la seguridad, que se ha adaptado rápidamente a las posibilidades que ofrece la tecnología moderna. En este sentido, el ciberespacio juega hoy un papel más relevante a nivel de espionaje y es utilizado por Estados, grupos o individuos que usan sofisticados programas que proporcionan acceso a ingentes volúmenes de información y datos sensibles». [16]

Además, en el Informe Anual de Seguridad Nacional de 2019 se destaca la ciberseguridad como uno de los pilares fundamentales para la Seguridad Nacional. Así, este informe manifiesta lo siguiente:

«El ciberespacio se consolida como entorno de relevancia estratégica, geopolítica, económica, social e individual con importantes implicaciones para la Seguridad Nacional.

Es un ámbito sin fronteras ni nítidas demarcaciones jurisdiccionales, de débil regulación, más allá de los códigos de buenas prácticas sobre comportamiento responsable, donde resulta difícil la trazabilidad y atribución de las acciones delictivas llevadas a cabo con diferentes objetivos tanto por actores estatales —o sus posibles intermediarios—, como no estatales —organizaciones terroristas, hacktivistas y grupos de ciberdelincuencia organizada—, dada la fácil accesibilidad a un amplio abanico de técnicas y la extensión del cibercrimen como modelo de negocio»[17].

[16] Estrategia de Seguridad Nacional 2017. Págs. 62-63. Disponible [en línea]: https: / / www.dsn.gob.es/ sites/ dsn/ files/ Estrategia de Seg-uridad_Nacional_ESN%20Final.pdf

[17] Informe Anual de Seguridad Nacional 2019. P.77. Disponible [en línea]: https: / / www.dsn.gob.es/ sites/ dsn/ files/ MASTER%20IASN2019 %2OWEB 0.pdf

cve: BOCG-14-CG-A-105

A la luz de lo anterior, resulta evidente que el ciberespionaje que pudieran desarrollar en España compañías extranjeras a través de nuestra red de 5G, especialmente proveedores tecnológicos chinos controlados por el propio Gobierno opresor chino, supone un riesgo para la Seguridad Nacional de España que debe de ser, cuanto menos, prevenido. Así, España debería evitar por todos los medios conceder la explotación de nuestras redes de telecomunicaciones a proveedores de opacidad manifiesta, controlados por Estados con fines espurios en nuestras propias redes.

En virtud de todo lo expuesto anteriormente, el Grupo Parlamentario VOX presenta la siguiente

Proposición no de Ley

«El Congreso de los Diputados insta al Gobierno de la Nación a llevar a cabo todas las acciones pertinentes para impedir, al amparo de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, la participación en la red española de 5G a cualquier proveedor tecnológico chino que se encuentre en los listados (entity list) del Departamento de Defensa y de Comercio de los Estados Unidos de América, o que sea sospechoso de estar bajo la influencia directa o indirecta de China, al objeto de impedir el ciberespionaje y, por ende, prevenir el riesgo que este tipo de acciones supone para los intereses estratégicos y de Seguridad Nacional de España.»

Palacio del Congreso de los Diputados, 22 de enero de 2021.—**Víctor González Coello de Portugal y Julio Utrilla Cano,** Diputados.—**Macarena Olona Choclán,** Portavoz del Grupo Parlamentario VOX.

161/001949 (CD)
663/000083 (S)

La Mesa del Congreso de los Diputados, en su reunión del día de hoy, ha adoptado el acuerdo que se indica respecto al asunto de referencia.

(161) Proposición no de Ley en Comisión.

Autor: Grupo Parlamentario VOX

Proposición no de Ley relativa a llevar a cabo todas las acciones diplomáticas que sean necesarias con el fin de promover que el Reino Unido cese la utilización de la base naval de Gibraltar como taller o refugio de submarinos nucleares, atendiendo a la grave amenaza que esta situación supone para la Seguridad Nacional de España.

Acuerdo:

Considerando que se solicita el debate de la iniciativa en Comisión, y entendiendo que es la Comisión Mixta la que insta al Gobierno a la adopción de las medidas correspondientes, admitirla a trámite como Proposición no de Ley, conforme al artículo 194 del Reglamento, y disponer su conocimiento por la Comisión Mixta de Seguridad Nacional. Asimismo, dar traslado del acuerdo al Gobierno, al Senado, al Grupo proponente y publicar en el Boletín Oficial de las Cortes Generales.

En ejecución de dicho acuerdo, se ordena la publicación.

Palacio del Congreso de los Diputados, 2 de febrero de 2021.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

A la Mesa del Congreso de los Diputados

D.ª Macarena Olona Choclán, D. Víctor González Coello de Portugal, D. Agustín Rosety Fernández de Castro y D. Julio Utrilla Cano, en sus respectivas condiciones de Portavoz Adjunta y Diputados del Grupo Parlamentario VOX (GPVOX), al amparo de lo establecido en el artículo 193 y siguientes del vigente Reglamento del Congreso de los Diputados, presentan la siguiente Proposición no de Ley relativa a llevar a cabo todas las acciones diplomáticas que sean necesarias con el fin de promover que el Reino Unido

cve: BOCG-14-CG-A-105

cese la utilización de la base naval de Gibraltar como taller o refugio de submarinos nucleares, atendiendo a la grave amenaza que esta situación supone para la Seguridad Nacional de España, para su discusión en la Comisión Mixta de Seguridad Nacional.

Exposición de motivos

Primero. A efectos de contextualizar la ya de sobra conocida situación geopolítica particular de Gibraltar, cabe destacar que el Peñón, desde los años sesenta, figura en el listado de las Naciones Unidas como uno de los «territorios no autónomos pendientes de descolonización». Por su parte, resulta imperativo señalar que este vestigio colonial destruye la unidad nacional y la integridad territorial de España, además de contravenir lo establecido en la Resolución 1514 (XV) 1960, sobre descolonización[1]. En este sentido, España ha solicitado reiteradamente al Reino Unido entablar negociaciones, en cumplimiento de lo dispuesto por las Naciones Unidas, para llegar a una solución definitiva del contencioso de Gibraltar, única colonia existente en Europa.

Así, de acuerdo con el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, Naciones Unidas ha señalado reiteradamente que «en el proceso de descolonización de Gibraltar, el principio aplicable no es el de libre determinación de los pueblos sino el de restitución de la integridad territorial española. La cuestión de Gibraltar debe ser resuelta mediante negociaciones bilaterales entre España y el Reino Unido. La ONU ha venido recomendando estas negociaciones, ininterrumpidamente, desde 1965»[2].

Por su parte, la situación conflictiva entre España y el Reino Unido por la soberanía del Peñón tiene su origen en el Tratado de Utrecht, firmado por ambas naciones en 1713, como solución pacífica a la Guerra de Sucesión Española.

En concreto, mediante la firma del Tratado de Utrecht, España cedía a la Gran Bretaña «la ciudad y el castillo de Gibraltar junto con su puerto, defensas y fortalezas que le pertenecen» [3]. No obstante, el istmo (como las aguas adyacentes o el espacio aéreo supra yacente) no fue cedido por España, quedando siempre éste bajo soberanía española. Además, el artículo X del citado tratado recoge tres condiciones en las que se encuadra la cesión, siendo las siguientes:

1) Se define el territorio cedido como la ciudad y castillo de Gibraltar, juntamente con su puerto, defensas y fortalezas que le pertenecen, sin plazo de tiempo, pero «sin jurisdicción alguna territorial».

2) No se permite la «comunicación abierta con el país circunvecino por tierra», salvo para el abastecimiento en caso de necesidad.

3) España tiene un derecho a «redimir» la ciudad de Gibraltar, es decir, recuperar su soberanía, en caso de que Gran Bretaña quiera «dar, vender o enajenar de cualquier modo» su propiedad.

En vista de lo anterior, la mera ocupación de facto continuada por los británicos del istmo y de las aguas adyacentes contraviene las condiciones acordadas en el Tratado de Utrecht para la adquisición de soberanía sobre ese territorio, —por limitarse la cesión de soberanía únicamente a la ciudad y castillo de Gibraltar, juntamente con su puerto, defensas y fortalezas—, además de resultar ilegítima con arreglo al Derecho Internacional. Por eso, España siempre ha señalado que la ocupación del istmo es ilegal e ilegítima y, por tanto, ha reclamado siempre su devolución sin condiciones.

Por si esto no fuera suficiente, la intención del Reino Unido de dar un nuevo estatuto jurídico a Gibraltar fuera del marco descolonizados supone una acción de las previstas en el Tratado de Utrecht que habilitarían a España a redimir la ciudad de Gibraltar, como se ha citado anteriormente. Así, la insistencia en la promesa unilateral del Reino Unido de atender a la voluntad de los gibraltareños de adquirir su propia autonomía implicaría, tácitamente, la «enajenación» de la propiedad británica.

Pese a que esa enajenación no se realizaría con respecto a otra potencia o Estado, sino con respecto a la propia población de Gibraltar, «la retrocesión a España no depende según el Derecho Internacional de esa voluntad local sino de la decisión de Gran Bretaña de cambiar el régimen de la propiedad de cualquier modo»[4].

---

[1] Resolución 15141XV), Declaración sobre la concesión de la independencia a los países y pueblos coloniales, punto 6. 14 de diciembre de 1960. Disponible [en lineal: http: / /undocs.org/ es/ A/ Res/ 1514(XV)

[2] Extraído de la página web del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. httpl /www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Gibraltar/Paginas/Hist oria.aspx

[3] ORTEGA CARCELÉN, MARTÍN. Gibraltar y el Tratado de Utrecht. Real Instituto Elcano.

[4] Ibid.

cve: BOCG-14-CG-A-105

Segundo. Además de encontrarse respaldada por la legalidad internacional para la justa reclamación de la soberanía sobre Gibraltar, la posición española encuentra, por otra parte, motivos suficientes para considerar Gibraltar como un asunto de interés vital para la Seguridad Nacional de España. Así, según informaciones publicadas en prensa «la Armada británica intensifica su presencia en Gibraltar. En el último tramo de las negociaciones con España sobre el estatus del Peñón tras el Brexit coincide con un incremento de la actividad de la base que Londres mantiene en la última colonia de Europa»[5].

Así pues, el 16 de noviembre de 2020 salió de la base naval de Gibraltar el HMS Kent (F78), una fragata de la clase Duke de 133 metros de eslora que realizó «ejercicios de superficie con maniobras de alta velocidad» en aguas que se encuentran actualmente bajo soberanía en disputa entre España y el Reino Unido, y en los que también participó el buque HMS Pursuer (P273). Adicionalmente, poco después que el HMS Kent realizara sus ejercicios de maniobra, «hizo entrada en Gibraltar un barco de guerra de casi el doble de tonelaje, el HMS Dragon (D35), un destructor de última generación especializado en defensa aérea de la clase Daring y 155 metros de eslora»[6].

Sin embargo, estos no han sido los únicos atraques de buques militares en Gibraltar. A finales de noviembre, «El submarino nuclear USS Seawolf [volvió] a Gibraltar y, esta vez, ha entrado a puerto donde previsiblemente será sometido a algún tipo de reparación, teniendo en cuenta las evoluciones anteriores tanto del sumergible como de los aviones militares que han llegado al Peñón»[7].

Estos hechos confirman la utilización de Gibraltar como «taller de reparaciones para submarinos nucleares británicos y estadounidenses»[8]. Por tanto, con este tipo de actuaciones, se confirma que Gibraltar pone en riesgo de sufrir las consecuencias de un accidente nuclear a los españoles que viven en la comarca del Campo de Gibraltar.

De hecho, resulta razonable afirmar que Gibraltar es en sí mismo una base militar. Así, «Al norte, en el istmo —ocupado ilegalmente— está el aeródromo de la RAF. Al sur, las instalaciones de Inteligencia (también contra España) y de control del tráfico del Estrecho. En el puerto (comercial y militar) está la base naval, con un muelle en el que reparan submarinos nucleares, del RU y de EE. UU. En lo alto del Peñón están las antenas de radar y las de comunicaciones. En los túneles almacenan munición de artillería naval, bombas, minas, misiles, torpedos e incluso material radiactivo»[9].

No obstante lo anterior, resulta imprescindible señalar que, como se ha expuesto anteriormente, tanto la base naval de Gibraltar como las aguas que hoy rodean el puerto o muelle construido por los británicos (o, en otras palabras, todo lo que no se circunscriba única y exclusivamente a la ciudad y castillo de Gibraltar, juntamente con su puerto, defensas y fortalezas) es territorio español con arreglo al Derecho Internacional. Por tanto, todos los buques de guerra que permanecen actualmente atracados en dichas aguas, así como todos los barcos que entran y salen del puerto de Gibraltar, incluidos los submarinos nucleares que arriban a dichas aguas para ser reparados o refugiarse, lo están haciendo en territorio español. Aún pese a que el Reino Unido considere esas aguas como propias.

En atención a lo anterior, la presencia de submarinos nucleares en las aguas de Gibraltar supone un fuerte conflicto con la política nacional española en materia nuclear. Esto es así ya que España se autoimpone un uso muy restrictivo de la energía nuclear dentro de su territorio, la cual está prevista únicamente con fines civiles. Además, la Estrategia de Seguridad Nacional contempla, dentro del objetivo de «No proliferación de armas de destrucción masiva», una línea de acción para «garantizar la seguridad física de los materiales e instalaciones nucleares y radiactivos» [10].

Este último punto es el que reviste más relevancia, puesto que la presencia de dichos submarinos en territorio español afecta a la propia Seguridad Nacional de España.

Tercero. En vista de lo anterior, la situación actual del Peñón de Gibraltar se erige como el mayor punto de fricción entre el Reino Unido y el Reino de España. Dos países socios, aliados y amigos, que

---

[5] ROJO, A.: «La Armada británica intensifica su presencia en Gibraltar», La Razón, 17/11/2020. https: / / www.larazon.es / espana/ 20201117/ falarchalj ge3hv dh4m6jiz3cy.html

[6] Ibid.

[7] «El submarino nuclear USS Seawolf, en Gibraltar para probables reparaciones», noticiasgibraltar, 01.12.2020. https: / / noticiasgibraltar.es / gibraltar / noticias /submarino-nuclear-uss-seawolfgibraltar-para-probables-reparaciones

[8] Ibídem.

[9] https: / / amp.heraldo.es/ noticias/ opinion/ 2021/ 01/ 18 /una-base-britanica-en-la-ue-angelliberal-fernandez-la-firma-1414988.html

[10] Estrategia de Seguridad Nacional de 2017, P. 94-95.
https://www.dsn.gob.es/sites/dsn/files/Estrategia de Seguridad Nacional ESN%20Final.pdf

cve: BOCG-14-CG-A-105

mantienen una antiquísimas relaciones bilaterales que suponen un pilar fundamental para la estabilidad de Occidente.

Por tanto, aunque el Reino de España debe ser consciente de la relevancia que Gibraltar supone para el Reino Unido en materia de seguridad y defensa, no es posible obviar el hecho de que está en juego tanto la integridad territorial española como la Seguridad Nacional de la región.

En cuanto al primer concepto, cabe resaltar su carácter de elemento especialmente protegido por nuestra Constitución, además de por la doctrina de Naciones Unidas, la cual, en la ya citada Resolución 1514 (XV), señala que «Todo intento encaminado a quebrantar total o parcialmente [...] la integridad territorial de un país es incompatible con los propósitos y principios de la Carta de Naciones Unidas» [11]. Adicionalmente, tal y como queda patente según los términos acordados en el Tratado de Utrecht, España está amparada por el Derecho Internacional para recuperar la soberanía sobre el Peñón ante el grave incumplimiento por parte del Reino Unido de las condiciones pactadas en ese mismo tratado.

Por otro lado, el hecho de que el Reino Unido esté utilizando territorio español como taller o refugio de submarinos nucleares supone una grave amenaza para la Seguridad Nacional de España, en general, y para la seguridad de los ciudadanos españoles que habitan la región, en particular. Lo anterior es así por cuanto que, como se ha expuesto, las aguas de Gibraltar pertenecen legítimamente a España, por lo que el atraque de submarinos nucleares de una potencia extranjera supone no sólo una afrenta a la soberanía española sobre dicho territorio, sino también un riesgo directo para la Seguridad Nacional, ya que España no tiene la posibilidad de monitorizar ni controlar de forma alguna la actividad realizada por o sobre dichos submarinos nucleares que se encuentran dentro de su propio territorio.

Por todo ello, y al amparo de lo expuesto anteriormente, el Grupo Parlamentario VOX presenta la siguiente

Proposición no de Ley

«El Congreso de los Diputados insta al Gobierno de la Nación a llevar a cabo todas las acciones diplomáticas que sean necesarias con el fin de promover que el Reino Unido cese en la utilización de la base naval de Gibraltar como taller o refugio de submarinos nucleares, atendiendo a la grave amenaza que esta situación supone para la Seguridad Nacional de España, y al hecho de que dichos submarinos se refugian o están siendo reparados en territorio español con arreglo al Derecho Internacional.»

Palacio del Congreso de los Diputados, 25 de enero de 2021.—**Víctor González Coello de Portugal, Julio Utrilla Cano y Agustín Rosety Fernández de Castro,** Diputados.—**Macarena Olona Choclán,** Portavoz del Grupo Parlamentario VOX.

Comisión Mixta para la Unión Europea

161/001959 (CD)
663/000084 (S)

La Mesa del Congreso de los Diputados, en su reunión del día de hoy, ha adoptado el acuerdo que se indica respecto al asunto de referencia.

(161) Proposición no de Ley en Comisión.

Autor: Grupo Parlamentario Ciudadanos.

Proposición no de Ley sobre la utilización responsable de los fondos Next Generation EU y la agenda de reformas estructurales.

[11] Resolución 1514 (XV), Declaración sobre la concesión de la independencia a los países y pueblos coloniales, punto 6. 14 de diciembre de 1960. Disponible [en línea]: http: / / undocs. org/ es/ A/ Res/ 1514(XV)

cve: BOCG-14-CG-A-105

Acuerdo:

Considerando que se solicita el debate de la iniciativa en Comisión, y entendiendo que es la Comisión Mixta la que insta al Gobierno a la adopción de las medidas correspondientes, admitirla a trámite como Proposición no de Ley, conforme al artículo 194 del Reglamento, y disponer su conocimiento por la Comisión Mixta para la Unión Europea. Asimismo, dar traslado del acuerdo al Gobierno, al Senado, al Grupo proponente y publicar en el Boletín Oficial de las Cortes Generales.

En ejecución de dicho acuerdo, se ordena la publicación.

Palacio del Congreso de los Diputados, 2 de febrero de 2021.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

A la Mesa del Congreso de los Diputados

El Grupo Parlamentario Ciudadanos, al amparo de lo establecido en el artículo 193 y siguientes del vigente Reglamento del Congreso de los Diputados, presenta la siguiente Proposición no de Ley sobre la utilización responsable de los fondos Next Generation EU y la agenda de reformas estructurales, para su debate en la Comisión Mixta para la Unión Europea.

Exposición de motivos

Las instituciones de la Unión Europea, Consejo, Parlamento y Comisión finalizaron en las últimas semanas el Reglamento que regirá el funcionamiento de los fondos europeos para paliar las consecuencias del COVID-19 y que, previsiblemente, se aprobará definitivamente en febrero. Entre las consideraciones que se reflejan en este documento, destaca la condicionalidad que muchas veces se ha mencionado por parte de algunos países miembros y de varios grupos parlamentarios, con el ánimo de que estos fondos contribuyan a fortalecer los pilares de los sistemas económico y social de los países receptores.

Según este reglamento, los países miembros deberán remitir a Bruselas un plan de reformas estructurales con hitos y metas que será evaluado por la Comisión y recibirá una nota. Esta evaluación determinará el desembolso de los fondos, a excepción del primer 13 % que será incondicional. El Plan de Reformas debe contener los mecanismos y objetivos para conseguir reducir los desafíos y prioridades identificadas en el procedimiento del Semestre Europeo y así mismo incluir los aspectos fiscales y las recomendaciones hechas a los países bajo el amparo del Artículo 6 del Reglamento 1176/2011 de prevención y corrección de los desequilibrios macroeconómicos. Sobre estos principios generales, la Comisión evaluará específicamente la contribución del plan a los siguientes pilares: la mejora del crecimiento potencial, la creación de empleo y actividad económica, la resiliencia social e institucional del país miembro, la promoción de políticas dirigidas a los jóvenes que mitiguen el impacto social y económico de la crisis, la contribución al Pilar Europeo de Derechos Sociales, el impulso de la cohesión y convergencia económica, social y territorial dentro de la Unión, y el plan para que estos objetivos no dañen el medioambiente en consonancia con el Artículo 17 del Reglamento 2020/852.

Bajo el paraguas de los fondos europeos, el desembolso se hará de acuerdo al cumplimiento de las metas establecidas en el plan de reformas que se determinará recabando la opinión del Comité Económico y Financiero basado en el análisis preliminar del desempeño del país en cuestión elaborado por la Comisión. Además, si uno o más países creen que hay desviaciones significativas del plan presentado por el país analizado, pueden referir la decisión de desembolso al Consejo Europeo donde el asunto será discutido en profundidad.

El Reglamento, además, es claro en relación con el destino de los fondos, que no podrán ser empleados para sustituir gastos corrientes de la Administración.

Todo lo anterior, da una muestra de los retos a los que se enfrentará el Gobierno para llevar a cabo las reformas estructurales que necesita nuestro país y que, desde Ciudadanos siempre hemos defendido y que, de no acometerse, podrían ser una gran pérdida para España ya que eso supondría que nuestro país pierde la condición de receptor de los fondos europeos. Así lo reflejamos también en las enmiendas que presentamos al proyecto de ley de Presupuestos Generales del Estado para 2021, que aspiraban a asegurar un uso responsable de los fondos europeos del paquete Next Generation EU, siempre de acuerdo con las recomendaciones hechas a España en el seno del Semestre Europeo, y que fueron rechazadas por los grupos parlamentarios que apoyan al Gobierno.

cve: BOCG-14-CG-A-105

Por todo ello, el Grupo Parlamentario Ciudadanos presenta la siguiente

Proposición no de Ley

«Se insta al Gobierno a garantizar que la utilización de fondos europeos del paquete Next Generation EU tendrá como objetivo la puesta en marcha de las reformas estructurales contenidas en las recomendaciones del Semestre Europeo respecto a los siguientes puntos:

1. En materia laboral, la lucha contra la precariedad laboral —especialmente entre los jóvenes—, la eliminación de la dualidad del mercado laboral, el establecimiento de incentivos a la contratación y la reinserción laboral de desempleados de larga duración.
2. En materia fiscal, la revisión del sistema impositivo para establecer un régimen fiscal más favorable al crecimiento, la inversión privada y la competitividad, reduciendo impuestos al trabajo y al capital y sustituyéndolos por impuestos a actividades perjudiciales.
3. En materia económica, la eliminación de la fragmentación y las trabas burocráticas que impiden a las empresas beneficiarse de las economías de escala y afectan negativamente a la productividad, garantizando una coordinación reforzada y sostenida entre los distintos niveles de gobierno para aumentar la eficacia de las políticas encaminadas a facilitar la recuperación.
4. En materia de gasto público, garantizar la sostenibilidad de las cuentas públicas mediante la contención del gasto público primario neto por debajo del 0,9 % y un ajuste estructural anual del 0,65 % en el momento en que dejen de aplicarse medidas de salvaguarda, destinando ingresos extraordinarios a la reducción de la ratio de deuda pública.
5. En materia de pensiones, preservar la sostenibilidad del sistema de pensiones mediante los incentivos a complementar la prestación pública con un sistema de ahorro alternativos y facilitando la creación de empleo entre los jóvenes.
6. En materia educativa y de formación, reforzar la orientación educativa en particular a los estudiantes con algún tipo de desventaja o en situación de vulnerabilidad, atendiendo de forma especial al sistema educativo en Comunidades Autónomas, municipios y distritos con peores resultados académicos y con una mayor tasa de abandono escolar temprano, y mejorando las competencias digitales de alumnos, docentes y trabajadores, también en zonas rurales.
7. En materia de innovación, mejorar los incentivos a la cooperación público-privada y establecer un sistema más ambicioso de incentivos fiscales para fomentar la inversión empresarial en innovación, incluyendo medidas para la atracción y retención de talento.
8. En materia institucional, el refuerzo de la separación de poderes y la independencia del poder judicial, mejorando su eficiencia; la eliminación de trabas burocráticas y procedimientos repetitivos en la contratación pública y la cooperación público-privada, y el refuerzo de la prevención, control y sanción de conductas fraudulentas.
9. En materia climática y de energía, la inversión en renovaciones a gran escala de edificios públicos y privados para mejorar la eficiencia energética, el desarrollo de redes inteligentes para mejorar los patrones de consumo de las familias, y la promoción de fuentes de energía renovables y de emisiones cero como motor de la creación de empleo.
10. En materia ambiental, invertir en la conservación de ecosistemas, en las soluciones para prevenir y paliar los efectos adversos del cambio climático como olas de calor, inundaciones, incendios forestales y otros fenómenos extremos, así como en las mejoras de la calidad del aire, de la gestión de recursos hídricos y de los residuos, y en el desarrollo de la economía circular a nivel industrial y de consumidores particulares.»

Palacio del Congreso de los Diputados, 26 de enero de 2021.—**Marta Martín Llaguno,** Diputada.—**Inés Arrimadas García,** Portavoz del Grupo Parlamentario Ciudadanos.

cve: BOCG-14-CG-A-105

PREGUNTAS PARA RESPUESTA ORAL

Comisión Mixta de Seguridad Nacional

681/000816 (S)
181/000680 (CD)

La Mesa de la Cámara, en su reunión del día 26 de enero de 2021, ha adoptado el acuerdo que se indica respecto al asunto de referencia.

Pregunta oral en Comisión.

Autor: Márquez Sánchez, Francisco Javier (GPP).

Pregunta sobre el número de ciberataques constatados por el Gobierno durante el año 2020, con indicación de los considerados como graves.

Acuerdo:

Admitir a trámite, conforme a lo dispuesto en el artículo 168 del Reglamento del Senado y encomendar su conocimiento a la Comisión Mixta de Seguridad Nacional; asimismo, dar traslado al Gobierno, al Congreso de los Diputados, notificar este acuerdo a su autor y publicar en el Boletín Oficial de las Cortes Generales (Sección Cortes Generales).

En consecuencia se ordena la publicación en la Sección Cortes Generales del BOCG, de conformidad con lo establecido en el Acuerdo de las Mesas del Congreso de los Diputados y del Senado de 19 de diciembre de 1996.

Palacio del Senado, 26 de enero de 2021.—P.D. El Letrado Mayor del Senado, **Manuel Cavero Gómez.**

A la Presidencia del Senado

Don Francisco Javier Márquez Sánchez, Senador por Jaén del Grupo Parlamentario Popular, al amparo de lo previsto en los artículos 160, 168 y siguientes del Reglamento de la Cámara, tiene el honor de presentar la siguiente pregunta al Gobierno, para la que desea obtener respuesta oral en la Comisión de Mixta Seguridad Nacional.

¿Cuántos ciberataques ha constatado el Gobierno de España que ha sufrido tanto el sector público como el privado español durante el año 2020 y cuantos de ellos han sido constatados como graves?

Palacio del Senado, 20 de enero de 2021.—**Francisco Javier Márquez Sánchez,** Senador.

681/000817 (S)
181/000681 (CD)

La Mesa de la Cámara, en su reunión del día 26 de enero de 2021, ha adoptado el acuerdo que se indica respecto al asunto de referencia.

Pregunta oral en Comisión.

Autor: Márquez Sánchez, Francisco Javier (GPP).

Pregunta sobre las medidas y acciones concretas adoptadas por el Gobierno durante el año 2020 para ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas.

cve: BOCG-14-CG-A-105

Acuerdo:

Admitir a trámite, conforme a lo dispuesto en el artículo 168 del Reglamento del Senado y encomendar su conocimiento a la Comisión Mixta de Seguridad Nacional; asimismo, dar traslado al Gobierno, al Congreso de los Diputados, notificar este acuerdo a su autor y publicar en el Boletín Oficial de las Cortes Generales (Sección Cortes Generales).

En consecuencia se ordena la publicación en la Sección Cortes Generales del BOCG, de conformidad con lo establecido en el Acuerdo de las Mesas del Congreso de los Diputados y del Senado de 19 de diciembre de 1996.

Palacio del Senado, 26 de enero de 2021.—P.D. El Letrado Mayor del Senado, **Manuel Cavero Gómez.**

A la Presidencia del Senado

Don Francisco Javier Márquez Sánchez, Senador por Jaén del Grupo Parlamentario Popular, al amparo de lo previsto en los artículos 160, 168 y siguientes del Reglamento de la Cámara, tiene el honor de presentar la siguiente pregunta al Gobierno, para la que desea obtener respuesta oral en la Comisión Mixta Seguridad Nacional.

¿Qué medidas y acciones concretas se han adoptado por el Gobierno de España durante el año 2.020 para ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas con el fin de permitir la identificación de procedimientos y orígenes de ataque, así como la elaborar la inteligencia necesaria para una protección, atribución y defensa más eficaz?

Palacio del Senado, 20 de enero de 2021.—**Francisco Javier Márquez Sánchez,** Senador.

---

cve: BOCG-14-CG-A-105