BOLETÍN OFICIAL
DE LAS CORTES GENERALES

# SECCIÓN CORTES GENERALES

XIV LEGISLATURA

**Serie A:**
**ACTIVIDADES PARLAMENTARIAS** **27 de abril de 2021** **Núm. 131** **Pág. 1**

## ÍNDICE



cve: BOCG-14-CG-A-131

# CONTROL DE LA ACCIÓN DEL GOBIERNO

PROPOSICIONES NO DE LEY/MOCIONES

## Comisión Mixta para la Unión Europea

**161/002387 (CD)**
**663/000105 (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 Euskal Herria Bildu.

Proposición no de Ley sobre liberalización temporal de las patentes de las vacunas contra la COVID-19.

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, 20 de abril 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 Euskal Herria Bildu, a instancia de Gorka Elejebarrieta, al amparo de lo establecido en el artículo 193 y siguientes del Reglamento de la Cámara, presenta la siguiente Proposición no de Ley sobre liberalización temporal de las patentes de las vacunas contra la COVID-19 para su debate en la Comisión Mixta para la Unión Europea.

Exposición de motivos

Nos encontramos ante una crisis sanitaria global que requiere de soluciones globales. Frente a la pandemia generada por el COVID-19 que ya se ha cobrado más de 2,5 millones de vidas, las vacunas suponen la mayor esperanza para que el mundo, todos los países y sus sociedades, puedan acabar con la pandemia. Las vacunas son por tanto, un bien común global que debería ser accesible a todo el mundo lo antes posible.

Pero lejos de alcanzar este objetivo, la disponibilidad de las vacunas es hoy limitada e insuficiente. Su producción se concentra en unas pocas empresas farmacéuticas y su distribución es acaparada por países ricos. Esto está provocando una desigual distribución e inoculación entre países, limitando el acceso a las vacunas solo a los países que disponen de capacidad económica y recursos suficientes para poder costearlas, dando paso a la especulación por parte de las farmacéuticas que ostentan el monopolio de la producción.

Según Médicos Sin Fronteras, nueve de cada diez personas de países del Sur global, no recibirán la vacuna de la COVID-19 en 2021. Según el Centro de Innovación en Salud Global de la Universidad de Duke, más de la mitad de las vacunas las han adquirido países enriquecidos, que tan solo suman el 14 % de la población mundial. Esta situación es no solo tremendamente injusta e insolidaria, sino tremendamente peligrosa para todos los países.

cve: BOCG-14-CG-A-131

Porque como avisa la OMS, si no se inmuniza a la mayor parte de la población mundial posible en el menor tiempo posible, el virus mutará como ya está ocurriendo, y las vacunas podrían perder su efectividad. Por lo que todos, tanto las personas de los estados ricos como de los empobrecidos, volveremos a estar en peligro y la pandemia seguirá avanzando, como avanzarán sus terribles consecuencias sanitarias, sociales y económicas.

India y Sudáfrica solicitaron en octubre a la OMC suspender temporalmente, mientras dure la pandemia, la exención de determinadas obligaciones recogidas en los Acuerdos sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), es decir, las patentes para las vacunas. El propio acuerdo de la OMC estipula que se puede renunciar a las mismas en circunstancias excepcionales, y esta sin duda lo es. 100 países apoyaron la iniciativa, bastantes menos, pero más poderosos, incluyendo a Estados Unidos y la Unión Europea en su totalidad, se opusieron.

La exención propuesta por Sudáfrica y la India facilitaría la posibilidad de compartir la propiedad intelectual y el know-how. Permitiría compartir el conocimiento y la tecnología de las vacunas contra el COVID-19, permitiendo una colaboración que aumente y acelere la disponibilidad, accesibilidad y asequibilidad de las vacunas, pruebas y tratamientos para la COVID-19 a nivel mundial.

Aprobar esta liberalización temporal permitiría una producción de vacunas a escala global, una distribución a escala global y lo más importante, una inmunización a escala global. Supondría convertir las vacunas en un bien común global, evitando más contagios, más muertes y nuevas variantes que recrudecerían la pandemia. Por todo ello, se presenta la siguiente

Proposición no de Ley

«El Congreso de los Diputados insta al Gobierno de España a adoptar, ante la OMC y el Consejo Europeo, un posicionamiento favorable del Estado Español a la liberalización temporal de las patentes de las vacunas contra la COVID-19, permitiendo una colaboración que aumente y acelere la disponibilidad, accesibilidad y asequibilidad de las vacunas».

Palacio del Congreso de los Diputados, 8 de abril de 2021.—**Gorka Elejebarrieta Díaz,** Senador.—**Oskar Matute García de Jalón,** Portavoz del Grupo Parlamentario Euskal Herria Bildu.

---

**161/002392 (CD)**
**663/000106 (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 instar, en el seno de la Unión Europea, la adopción de todas aquellas medidas destinadas a aumentar la ciberseguridad de las redes e instituciones públicas de los Estados miembros frente a posibles ataques cibernéticos efectuados por parte de potencias o actores extranjeros.

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, 20 de abril de 2021.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

cve: BOCG-14-CG-A-131

A la Mesa del Congreso de los Diputados

Don Iván Espinosa de los Monteros de Simón, doña Macarena Olona Choclán, don José María Sánchez García, don Alberto Asarta Cuevas, don Víctor González Coello de Portugal y don Julio Utrilla Cano, en sus respectivas condiciones de Portavoz, 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, en el seno de la Unión Europea, la adopción de todas aquellas medidas destinadas a aumentar la ciberseguridad de las redes e instituciones públicas de los Estados miembros frente a posibles ataques cibernéticos efectuados por parte de potencias o actores extranjeros, para su discusión en la Comisión Mixta para la Unión Europea.

Exposición de motivos

Primero. El modo contemporáneo de «hacer la guerra» —también conocido como modern warfare—, ha difuminado la diferencia entre las acciones definitorias del conflicto armado de aquellas propias de relaciones pacíficas. Así pues, un aspecto relevante de esta «zona gris» es que, al desarrollarse por debajo del umbral bélico, «un actor puede desafiar a otro más poderoso militarmente, siguiendo un cálculo acorde con la paradoja estabilidad/inestabilidad: que un Estado posea el dominio de la escalada en un nivel del conflicto no impide —e incluso invita a— que sus rivales lleven la pugna a estratos inferiores» [1].

En este sentido, el investigador Javier Jordán, con estos argumentos, lo resume de la siguiente manera:

«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 y con objetivos a largo plazo» [2].

Siguiendo lo expuesto, el profesor Jordán también señala las líneas de acción estratégicas en la zona gris [3], esto es, los modos en los que la acción del Estado agresor se traduce:

I. Respaldo a la oposición política del Gobierno adversario para generar oposición, agudizar fracturas y perturbar sus procesos de toma de decisiones.

II. Operaciones de influencia sobre la opinión pública internacional y sobre la opinión pública del adversario, construyendo y difundiendo metanarrativas —en lo posible de manera encubierta, a través de terceros— ue afecten a los procesos políticos de otros Estados.

III. Coerción económica; mediante prácticas comerciales y financieras que refuercen la presión política. De nuevo se constata una gradación que va desde decisiones perfectamente legales y legítimas sobre la compra o venta de ciertos productos, a medidas de mayor calado como sanciones económicas o bloqueos.

IV. Ciberataques contra entidades públicas y privadas; que además de amedrentar y generar confusión en el proceso de toma de decisiones políticas, airean la vulnerabilidad del adversario. Pueden ser ataques de diversa consideración: desde denegaciones temporales de servicio en sitios web institucionales a acciones de mayor calado como los famosos ciberataques sufridos por Estonia en 2007 a manos de la Federación Rusa.

V. Acciones agresivas de inteligencia; las actividades de inteligencia de unos Estados sobre otros forman parte de la política normal pues por estrechas que sean las relaciones suele haber terrenos de competencia política o económica donde la inteligencia proporciona ventaja competitiva. Sin embargo, en la zona gris esas actividades se tornan más agresivas: numerosos intentos de infiltración de los servicios rivales, campañas extensivas de ciberespionaje de entidades públicas y privadas del rival, acoso y expulsión de agentes, etc.

[1] Jordan, Javier: «El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo», *Revista Española de Ciencia Política,* núm. 48,.2018. p. 131. Disponible [en línea]: https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf
[2] *Ibidem,* p. 133.
[3] *Ibidem,* pp. 137-141.

cve: BOCG-14-CG-A-131

VI. Disuasión militar coercitiva; Tradicionalmente en los estudios estratégicos coerción *(compellence)* y disuasión *(deterrence)* se han entendido como conceptos en cierto modo contrapuestos: amenaza o empleo limitado de la fuerza para que otro actor haga una cosa (coerción) o no haga otra (disuasión). Sin embargo, son complementarios pues dicha amenaza o empleo limitado de la fuerza puede incluir esa doble finalidad.

VII. Hechos consumados; obteniendo una determinada ganancia en un solo paso y sin intención de retroceder. Alteran súbitamente el *statu quo* y colocan al adversario en una posición incómoda: ya no se trata de que las cosas sigan como siempre, sino de forzar un retorno a la situación previa.

VIII. *Sliced salami tactics;* concatenando acciones de bajo perfil que proporcionan ganancias graduales y que a la vez dificultan una reacción severa por parte del adversario.

IX. Guerras por delegación *(proxy wars),* donde se apoya militarmente a un Gobierno o a un actor armado no estatal en contra de un rival estratégico.

Segundo. En efecto, estos modos de actuación en la zona gris tienen su aplicación práctica. Sin ir más lejos, en las últimas semanas hemos sido conocedores del ataque cibernético que ha sufrido el Servicio Público de Empleo Estatal (SEPE)[4], siendo este otro más de los ataques cibernéticos que sufren las instituciones públicas nacionales. Cabe recordar que el propio Ministerio de Defensa sufrió hace unos años una intrusión en su red informática[5].

Si bien todos los actores del tablero internacional que tienen la capacidad —es decir, el poder— de ejercer dichas actuaciones al final las acaban realizando, lo cierto es que algunos de estos están destacando por su asertividad.

Así pues, el creciente activismo de estas potencias revisionistas[6], unido a la cada vez menor confianza y voluntad de Occidente por defender el orden internacional liberal, está conduciendo a un deseo cada vez mayor de estas por cambiarlo. Este, y no otro, es el objetivo que estos países defienden y no tratan de ocultar[7].

En línea con lo anterior, no resulta sorprendente que los ataques que están sufriendo las instituciones públicas españolas sigan el patrón de actuación propio de esta nueva forma de hacer la guerra, es decir, contiene trazos característicos de las líneas de acción estratégicas de la zona gris. No obstante, resulta muy complicado atribuir la autoría de estos hechos —principal ventaja de estas actuaciones—. De hecho, la Agencia para Proyectos de Investigación Avanzada de Defensa (DARPA, por sus siglas en inglés) del Gobierno de los Estados Unidos de América, especifica que el mayor problema que detecta es la extrema dificultad de atribuir la autoría de actos maliciosos en el ciberespacio[8]. Así las cosas, es imperativo poder mejorar la capacidad de las instituciones a la hora de identificar a los autores de los ciberataques.

Tercero. Concretamente, y a modo de ejemplo, resulta imprescindible destacar los siguientes ataques sufridos por las instituciones españolas y que no pueden ni deben considerarse de forma aislada o como meras casualidades:

— En primer lugar, cabe recordar que en los días previos al referéndum ilegal en Cataluña del 1 de octubre del 2017, una avalancha de bots (programas informáticos controlados) invadieron la red para provocar una fuerte división política. Así pues, la Audiencia Nacional está investigando a un grupo vinculado a la inteligencia militar de un país extranjero por lanzar ataques informáticos y campañas en redes sociales para crear una confrontación entre partidarios y contrarios a la independencia con vistas a la votación, y así generar una desestabilización en España.

De hecho, según informaciones publicadas, el juez Manuel García-Castellón tiene abierta una investigación de la Comisaría General de Información de la Policía Nacional, tras una alerta del Centro

---

[4] Del Palacio, Guillermo: «Ataque al SEPE: ¿ Se pagarán las prestaciones por desempleo y ERTE?», *El Mundo,* 11.03.21. Disponible [en línea]: https://www.elmundo.es/economia/2021/03/11/604904e6fdddff975b8b4654.html

[5] «Defensa comunica a la Fiscalía un posible ataque a su red informática interna», *La Vanguardia,* 11.03.19. Disponible [en línea]: https://www.layanguardia.com/politica/20190311/46971060299/ministerio-defensacomunica-fiscalia-posible-ataque-red-informatica-interna.html

[6] Kagan, Robert: «Back into World War III», *Brookings,* 06.02.2017. Disponible [en línea]: https://www.brookings.edu/ research/backing-into-world-war-iii/

[7] De la Cal, Lucas: «China y Rusia hacen la pinza a EE. UU. y piden una reunión del Consejo de Seguridad de la ONU», *El Mundo,* 23.03.21. Disponible [en línea]: https://www.elmundo.es/internacional/2021/03/23/6059c5eefc6c83cc1e8b459d.html

[8] 2019 Strategic Framework, DARPA. Disponible [en línea]: https://www.darpa.mil/attachments/DARPA-2019-framework.pdf

cve: BOCG-14-CG-A-131

Nacional de Inteligencia (CNI), en relación con esta cuestión. Según fuentes de la investigación, España, y en concreto el conflicto catalán, es un contexto estratégico para llevar a cabo maniobras de desestabilización de Europa, después del Brexit en el Reino Unido [9].

— Por otra parte, y en relación con el ya mencionado ataque sufrido por el SEPE, cabe resaltar que tanto el Instituto Nacional de Ciberseguridad (INCIBE) como el Centro Criptológico Nacional (CCN), tienen la fuerte sospecha de que un país extranjero pudo haber estado detrás del ciberataque sufrido por este organismo público [10].

En ese sentido, el objetivo de un golpe como el sufrido por el SEPE es más bien desprestigiar a la institución pública y al Estado al que pertenece y suscitar el descontento de la ciudadanía por la cancelación de miles de citas en toda España y la paralización de la tramitación de nuevas prestaciones por desempleo especialmente en tiempos de crisis. Por tanto, solo una potencia que trate de ajustar cuentas con España puede estar interesada en inspirar tal ataque.

Cuarto. Así pues, ante el riesgo que supone para España —y, en general, para el resto de los países comunitarios—, la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. En efecto, tal y como se ha expuesto anteriormente, no pueden resultar casualidad los numerosos ataques que ha sufrido España durante los últimos tiempos, más si prestamos atención a las sospechas que tienen las instituciones públicas españolas dedicadas a la ciberseguridad —y las demás instituciones dedicadas a la salvaguarda de la Seguridad Nacional— de que nuestro país podría ser un objetivo prioritario de ataques cibernéticos.

Sin embargo, esta tan necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso tanto por parte del Gobierno español como de las instituciones comunitarias.

En vista de todo lo anterior y, en el actual contexto de competencia estratégica por el poder, Occidente (y en especial, España) debe hacer frente a las amenazas que el nuevo paradigma internacional conlleva, de tal forma que adopte una postura de alerta y prevención ante los crecientes movimientos desestabilizadores de potencias y actores extranjeros.

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 promover en el seno de la Unión Europea la adopción de todas aquellas medidas destinadas a aumentar la ciberseguridad de las redes e instituciones públicas de los Estados miembros frente a posibles ataques cibernéticos efectuados por parte de potencias o actores extranjeros, prestando especial atención a que la red nacional y las instituciones públicas españolas estén debidamente protegidas y cuenten con todos los elementos de ciberseguridad que sean necesarios al objeto de prevenir y combatir los posibles ataques cibernéticos que pudieran sufrir».

Palacio del Congreso de los Diputados, 5 de abril de 2021.—**José María Sánchez García, Alberto Asarta Cuevas, Víctor González Coello de Portugal y Julio Utrilla Cano,** Diputados.—**Iván Espinosa de los Monteros de Simón y Macarena Olona Choclán,** Portavoces del Grupo Parlamentario VOX.

[9] Guindal Madrid, Carlota: «Una avalancha de bots rusos invadió la red para aumentar la división política por el 1-O», *La Vanguardia,* 22.11.2019. Disponible [en línea]: https://www.lavang-uardia.com/ politica/ 20191122 / 471782579479 / bots-rusos-divisionpolitica-1-o.html

[10] Cembrero, Ignacio: «La inteligencia española sospecha que Rusia estuvo tras el ciberataque al SEPE», *El Confidencial,* 21.03.2021. Disponible [en línea]: https://www.elconfidencial.com/ espana/ 2021-03-21 /rusia-hackeo-sepe-inteligencia-esóana 3000291/

cve: BOCG-14-CG-A-131

PREGUNTAS PARA RESPUESTA ORAL

## Comisión Mixta de Seguridad Nacional

**181/000951 (CD)**
**683/000143 (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.

(181) Pregunta oral al Gobierno en Comisión.

Autor: Olona Choclán, Macarena (GVOX).

Actuaciones y actividad concreta que se está llevando a cabo por parte de la Comisión Permanente contra la Desinformación.

Acuerdo:

Admitir a trámite, conforme a lo dispuesto en el artículo 189 del Reglamento, y encomendar su conocimiento a la Comisión Mixta de Seguridad Nacional. Asimismo, dar traslado del acuerdo al Gobierno, al Senado 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, 20 de abril de 2021.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

A la Mesa del Congreso de los Diputados

Diputada: doña Macarena Olona Choclán, Grupo Parlamentario VOX.

Dirigida al Director del Gabinete de la Presidencia del Gobierno de España.

Texto:

En relación con la Comisión Permanente contra la Desinformación que dirige el Departamento de Seguridad Nacional, ¿podría indicar las actuaciones y actividad concreta que se está llevando a cabo por parte de esta comisión?

Palacio del Congreso de los Diputados, 24 de marzo de 2021.—**Macarena Olona Choclán,** Diputada.

---

**181/000997 (CD)**
**683/000144 (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.

(181) Pregunta oral al Gobierno en Comisión.

Autor: Olona Choclán, Macarena (GVOX).

Identidad de los miembros que componen la Comisión Permanente contra la Desinformación.

cve: BOCG-14-CG-A-131

Acuerdo:

Admitir a trámite, conforme a lo dispuesto en el artículo 189 del Reglamento, y encomendar su conocimiento a la Comisión Mixta de Seguridad Nacional. Asimismo, dar traslado del acuerdo al Gobierno, al Senado 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, 20 de abril de 2021.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

A la Mesa del Congreso de los Diputados

Diputada: doña Macarena Olona Choclán, Grupo Parlamentario VOX.

Dirigida al Director del Gabinete de la Presidencia del Gobierno de España.

Texto:

¿Podría indicar el Gobierno la identidad de los miembros que componen la Comisión Permanente contra la Desinformación?

Palacio del Congreso de los Diputados, 14 de abril de 2021.—**Macarena Olona Choclán,** Diputada.

cve: BOCG-14-CG-A-131