# *CIBERINJERENCIAS* EN PROCESOS ELECTORALES Y PRINCIPIO DE NO INTERVENCIÓN (UNA PERSPECTIVA INTERNACIONAL Y EUROPEA)

# *CYBER-INTERFERENCE IN ELECTORAL PROCESSES AND THE PRINCIPLE OF NON-INTERVENTION (AN INTERNATIONAL AND EUROPEAN PERSPECTIVE)*

**MARÍA JOSÉ CERVELL HORTAL***



RESUMEN: En los últimos años han proliferado las injerencias de Estados en procesos democráticos que se valen del ciberespacio para intentar cambiar el resultado electoral y/o manipular a los votantes. Este Estudio tiene como fin analizar el régimen jurídico aplicable a esas injerencias, más difíciles de detectar y de calificar jurídicamente, precisamente por tener lugar en ese entorno complejo (ciberespacio). Los esfuerzos más recientes de la Unión Europea para controlar este tipo de conductas son el punto de partida, pero este análisis se extiende también al Derecho Internacional y al sentir de los Estados en su conjunto, con especial atención a la aplicación de los principios de no intervención y soberanía en el ciberespacio. Afrontar las dificultades de la atribución de esas conductas y evaluar las respuestas posibles era el cierre final obligado de este artículo, que también se ocupa, por tanto, de las contramedidas y, en el caso de la UE, de las medidas restrictivas que podrían adoptarse.

*ABSTRACT: In recent years, there has been a proliferation of state interference in democratic processes using cyberspace to try to change the outcome of elections and/or manipulate voters. This Study aims to analyse the legal regime applicable to such interference, more difficult to detect and to qualify legally, because it takes place in that complex environment (cyberspace). The European Union's most recent efforts to control this type of conduct are the starting point of this analysis, which also studies the international law regime and the opinion of different states, with a special focus on the application of the principles of non-intervention and sovereignty to cyberspace. Tackling the difficulties of attributing such conduct and assessing possible reactions is the obligatory final closure of this article, which also deals with the countermeasures and, in the case of the EU, the restrictive measures that could be adopted*.

Fecha de recepción del trabajo: 22 de febrero de 2023. Fecha de aceptación de la versión final: 19 de abril de 2023.

* Catedrática de Derecho Internacional Público y Relaciones Internacionales, Universidad de Murcia, cervell@um.es. Este trabajo se ha desarrollado en el marco de los programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico del sistema de I+D+i orientada a los Retos de la Sociedad, convocatoria 2020, Proyecto PID2020-112577RB-I00 (*La búsqueda de una regulación internacional para las actividades cibernéticas ¿una ineludible necesidad?*), financiado por MCIN/AEI.

PALABRAS CLAVE: *ciberinjerencia*s electorales, ciberespacio, no intervención, soberanía, contramedidas, medidas restrictivas Unión Europea.

*KEYWORDS: electoral cyberinterference, cyberspace, non-intervention, sovereignty, countermeasures, EU restrictive measures.*

## I. INTRODUCCIÓN

No es nueva la preocupación que en los últimos años suscitan determinadas conductas que transcurren en el ciberespacio. En ese escenario en el que las fronteras físicas desaparecen, una vez relativamente superados los debates iniciales sobre si un Estado podía reclamar jurisdicción sobre él y si las normas del Derecho Internacional resultaban aplicables[1], es necesario replantearse la vigencia de otros conceptos que se consideraban ya, en algunos casos, asentados. Así ha ocurrido con las (ciber)injerencias en procesos democráticos, que obligan a cuestionarse la configuración tradicional de los principios de soberanía y de no intervención.

El intento de Rusia por interferir en el referéndum del Brexit en junio de 2016[2] fue el primer aviso claro de una tendencia que se incrementaría en los años siguientes: las elecciones presidenciales de Estados Unidos (2016)[3], de Francia (2016)[4] o el referéndum (ilegal) de independencia celebrado en Cataluña (2017)[5] demostraron el alcance e

[1] Sobre esas primeras discusiones, puede consultarse CERVELL HORTAL, Mª. J., *La legítima defensa en el Derecho contemporáneo (nuevos tiempos, nuevos actores, nuevos retos*), Aranzadi, Cizur Menor, 2017 (pp. 291-297, en las que se aborda directamente la cuestión del ciberespacio como nuevo escenario); GUTIÉRREZ ESPADA, C., "La ciberguerra y el Derecho internacional", en MARTÍNEZ PÉREZ, E. J. (coord.), MARTÍNEZ CAPDEVILA, C., ABAD CASTELOS, M. y CASADO RAIGÓN, R. (dirs.), *Las amenazas a la seguridad internacional hoy*, Tirant lo Blanch, Valencia, 2017, pp. 205-233 y, del mismo autor "Existe (ya) un Derecho aplicable a las actividades en el ciberespacio?", en CERVELL HORTAL, Mª. J. (dir.), *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio*, Aranzadi, Cizur Menor, 2020, pp. 225-248 (pp. 238-244); KETTEMAN, M. C., "Ensuring cybersecurity through international law", *Revista Española de Derecho Internacional*, vol. 69, 2, 2017, pp. 281-289 (p. 286) y SEGURA SERRANO, A. "Ciberseguridad y Derecho internacional", *Revista Española de Derecho Internacional*, vol 69, 2, 2017, pp. 291-299 (p. 292).

[2] Véase el denominado "Russia Report", Comité de Seguridad e Inteligencia del Parlamento británico, julio de 2020, *https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf*

[3] La implicación de Rusia fue formalmente declarada por la CIA estadounidense (*Assessing Russian Activities and Intentions in Recent US Elections*, 6 de enero de 2017, p. 2, https://www.dni.gov/files/documents/ICA_2017_01.pdf). Véase también el documento del Parlamento Europeo, "Kremlin trolls in the US presidential election", *At a glance*, European Parliamentary Research Service, February 2018, *https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/614700/EPRS_ATA(2018)614700_EN.pdf*

[4] Consúltese *https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/*

[5] A esa cuestión ya se refirió en 2021 el Informe del Comité del Parlamento Europeo sobre injerencia extranjera en todos los procesos democráticos de la UE, incluyendo la desinformación (doc. 2020/2268 INI, 18 de octubre de 2021, párr. BJ). También un Informe del Senado de Estados Unidos declaró esa injerencia: "Putin's asymmetric assault on democracy in Russia and Europe: implications for US national


DOI: 10.17103/reei.45.03

impacto que esas intervenciones podían tener, incluso respecto de Estados considerados democráticamente estables. Tampoco escapaban de ellas las elecciones al Parlamento Europeo de 2019[6], Estados Unidos volvía a sufrirlas en las presidenciales de 2020[7] y la sombra rusa sobrevoló igualmente la crisis del Gobierno italiano de Draghi de verano de 2022[8]. Rusia, China o Corea del Norte, principalmente, son el origen de ese tipo de operaciones, pero no pueden descartarse otros Estados e, incluso, actores no estatales[9].

La cuestión preocupa a los Estados en general, y también de manera particular a la Unión Europea, cuyo Parlamento aprobaba, el 9 de marzo de 2022, una resolución sobre "injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación"[10]. La resolución, que veía la luz tras 18 meses de trabajo y de consultas con 130 expertos, es el resultado final del esfuerzo acometido por un Comité Especial sobre injerencia en los procesos democráticos[11]. El Parlamento Europeo creaba unos días después (23 de marzo) un nuevo Comité sobre la misma cuestión, que ya continúa la labor de su predecesor y prepara iniciativas legales más concretas para acometer el problema[12].

Al hilo de los trabajos del Parlamento y de otras iniciativas europeas, este Estudio pretende analizar el régimen jurídico aplicable a las injerencias estatales que implican una violación del principio de no intervención, pero centrándose en una modalidad concreta:

---

security", The Committee on Foreign Relations, United States Senate, 10 de enero de 2018, pp. 133-136 (*https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf*).

[6] Véase *https://www.politico.eu/article/european-commission-disinformation-report-russia-fake-news/*

[7] El Director de la Inteligencia Nacional lo advirtió previamente en una declaración de 7 de agosto de 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

[8] Reuters, 25 de julio de 2022. También, el diario El Mundo de 28 de julio de 2022.

[9] El Parlamento europeo lo tiene claro: véase el documento *De un vistazo. Pleno de marzo de 2022*, disponible en https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729271/EPRS_ATA(2022)729271_ES.pdf. Sobre otros *ciberincidentes* electorales, consúltese "Understanding cybersecurity throughtout process: a reference document. A overview of cyber threats and vulnerabilities in elections", informe publicado por USAAID, DA e IFES, 2022, pp. 5-6, https://www.ifes.org/document/understanding-cybersecurity-throughout-electoral-process-reference-document-overview-cyber

[10] Doc. P0_TA(2022)0064, 9 de marzo de 2022. Operaciones de influencia (*ciberinjerencia*) y desinformación son dos conceptos próximos pero diferentes entre sí. Al respecto, TORRES SORIANO, M. R., "Operaciones de influencia vs. desinformación: diferencias y puntos de conexión", *Documento de Opinión 64/2022*, Instituto Español de Estudios Estratégicos, 28 de junio de 2022, pp. 1-16, pp. 3-4. Este trabajo no abordará, por razones de espacio, la desinformación, otra cuestión en la que la UE está trabajando intensamente y sobre la que también puede consultarse el documento de la Comisión "The strengthened Code of Practice on Disinformation", 2022, disponible en https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation y la publicación "1st EEAS Report on foreign information manipulation and interference threats. Towards a framework for networked defence", February 2023, en https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

[11] Creado por decisión del Parlamento Europeo de 18 de junio de 2020, doc. 2020/2683(RSO).

[12] Decisión del Parlamento Europeo, de 10 de marzo de 2022, sobre la constitución, competencias, composición numérica y duración del mandato de la Comisión Especial sobre injerencias extranjeras en todos los procesos democráticos de la UE, en particular la desinformación, doc. 2022/2585(RSO), párr. 7. (https://www.socialistsanddemocrats.eu/committees/special-committees-foreign-interference-all-democratic-processes-european-union).


DOI: 10.17103/reei.45.03

las que afectan directamente a procesos democráticos y tienen lugar en el ciberespacio, más complejas de detectar y con mayores problemas en cuanto a determinar qué normas son las aplicables. Aunque la resolución del Parlamento Europeo se tome como punto de partida y la normativa europea sea referencia obligada, el objeto de análisis se extenderá al régimen jurídico internacional, en tanto en cuanto la propia resolución remite a él. En concreto, se persigue aclarar cuándo las intromisiones en procesos electorales pueden calificarse de violaciones del principio de soberanía y de no intervención y qué respuestas están planteándose a nivel estatal y europeo. Quedan fuera, por tanto, de este análisis, las referencias a las posibles consecuencias que una *ciberinjerencia* en un proceso electoral pueda tener desde el punto de vista de los derechos humanos, así como otros problemas que afectan a la democracia como concepto y/o valor[13].

## II. ¿QUÉ ES LA *CIBERINJERENCIA* EN PROCESOS ELECTORALES Y POR QUÉ PREOCUPA A LA UNIÓN EUROPEA?

Las intromisiones en procesos democráticos adoptan multitud de formas, pero la mayoría de ellas se aprovechan de las redes sociales y el ciberespacio: *trolls* y *bots* que difunden ideas bajo perfiles falsos con el objetivo de condicionar el resultado de unas elecciones, pero también acciones que pretenden ofrecer información errónea en apoyo (o en contra) de determinados candidatos, programas electorales o miembros del Gobierno en el poder, con el fin de socavar su credibilidad. Son también frecuentes las filtraciones de correos electrónicos y los ataques contra páginas web de instituciones democráticas[14] o de partidos políticos[15]. Las sociedades democráticas se ven así sometidas a un desequilibrio constante y la polarización se multiplica, al tiempo que el Estado de Derecho se ve seriamente amenazado, pues se condicionan los procesos que lo garantizan. A veces, incluso, estas situaciones son el caldo de cultivo de otras más graves que, combinadas con elementos tradicionales (amenazas híbridas), podrían terminar generando conflictos de mayor envergadura, incluso de carácter armado.

[13] Hay al respecto muchos trabajos que pueden ilustrar al lector interesado en esas otras cuestiones: FRANCK, T. M., "Fairness in the International legal and institutional system. General Course on Public International Law", *RCADI*, vol. 240, 1993-III, pp. 9-498 (pp. 99-110); JARILLO ALDEANUEVA, A., *Pueblos y democracia en Derecho Internacional*, Tirant Monografías 792-UNED, Valencia, 2012, pp. 123-191 y ROTH, B. R., "Governmental illegitimacy in International Law", Oxford University Press, Oxford, 2000 (pp. 165-171). También, FOX, G. H., "The right to political participation in international law", en FOX, G. H. y ROTH, B. R., *Democratic governance and International Law*, Cambridge University Press, Cambridge, 2000, pp. 48-90; en la misma publicación, CRAWFORD, J., "Democracy and the body of international law", pp. 91-123 y REISMAN, W. M., "Sovereignty and human rights in contemporary international law", pp. 239-258 (pp. 250-253)

[14] De carácter masivo, como el sufrido por Estonia en 2007, o con objetivos más definidos, como los ciberataques que se dirigen directamente contra Parlamentos nacionales (por ejemplo, el llevado a cabo contra el *Bundestag* alemán en septiembre de 2021).

[15] *Https://www.politico.eu/article/us-russia-macron-campaign-hack-2017-election-france-attribution-gru/*


DOI: 10.17103/reei.45.03

La UE comenzó a trabajar en estas cuestiones con la Estrategia de Ciberseguridad de 2013[16], pero intensificó sus acciones después de la guerra de Ucrania (Crimea y Dombás) de 2014, a partir de la cual empezó a reconocer formalmente campañas de desinformación *online*. En 2015, el Consejo Europeo encargó al Alto Representante un Plan de Acción sobre Comunicaciones Estratégicas[17] que favoreció la creación del *East StratCom Task Force,*[18] encargado de controlar las campañas lanzadas desde Rusia sobre los Estados vecinos de la UE.

En 2016 se publica el "Comunicado conjunto sobre la lucha contra las amenazas híbridas: una respuesta de la UE", documento que resultó clave para atraer la atención sobre el tema y también para definir esas amenazas[19]. El "Informe relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas"[20], aprobado el año siguiente, incluía ya medidas concretas que los Estados podrían adoptar para prepararse ante este tipo de situaciones. En junio de 2018, un nuevo documento de la Comisión sobre la cuestión ("Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas"[21]) intentaba, a propuesta directa del Consejo Europeo, aumentar la capacidad preventiva y reactiva de la Unión frente a estos desafíos. En 2020 se aprobaba una nueva Estrategia para el Ciberespacio, alertando ya expresamente de las "amenazas híbridas que combinan campañas de desinformación con ciberataques a la infraestructura, los procesos económicos y las instituciones democráticas (…)". [22] En noviembre de 2022 se aprobaba la "Política de la UE sobre Ciberdefensa"[23], que contiene la estrategia de futuro para mejorar la seguridad en el ciberespacio.

Defenderse de la información falsa o distorsionada y proteger los procesos electorales se convertían en cuestiones que adquirían un protagonismo propio, tan comprensible como compatible con una coyuntura (crisis polaca y húngara) en la que la Unión Europea se volcaba en la protección (*ad intra*) del Estado de Derecho. La Comisión presentaba en 2018 su primer "Plan de Acción contra la Desinformacion"[24] y el "Plan de Acción de la

[16] Estrategia de Ciberseguridad de la UE: Un ciberespacio abierto, protegido y seguro, Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, doc. JOIN (2013) 1 final, 7 de febrero de 2013.

[17] *Https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf*

[18] El resultado de los trabajos que lleva a cabo ese Grupo puede consultarse en *https://euvsdisinfo.eu/*

[19] Comunicación conjunta al Parlamento Europeo y al Consejo sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea, doc. JOIN(2016) 18 final, 6 de abril de 2016, p. 2.

[20] Doc. JOIN(2017) 30 final, 19 de julio de 2017.

[21] Comunicación conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo, doc. JOIN(2018) 16 final, 13 de junio de 2018.

[22] Estrategia de Ciberseguridad de la UE para la Década Digital, Comunicación Conjunta al Parlamento Europeo y al Consejo, doc. JOIN(2020) 18 final, 16 de diciembre de 2020, p. 2.

[23] Comunicación Conjunta al Parlamento Europeo y al Consejo, Política de Ciberdefensa de la Unión Europea, doc. JOIN (2022) 49 final, 10 de noviembre de 2022. Previamente, el Consejo había dado el visto bueno en sus Conclusiones de 23 de mayo de 2022 (doc. 9364/22). Sobre el documento, PONTIJAS CALDERÓN, J. L., "Unión Europea: ciberseguridad y ciberdefensa", *Análisis 04/2023*, Instituto Español de Estudios Estratégicos, 20 de enero de 2023, pp. 1-14, pp. 5-6.

[24] Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, doc. JOIN(2018) 36 final, 5 de diciembre de 2018. Fruto de ese plan se aprobaba ese mismo año el *Código de Buenas Prácticas sobre la Desinformación*, compromiso


DOI: 10.17103/reei.45.03

Democracia Europea"[25]. Estas acciones se han visto, además, reforzadas por diversas normas de carácter preventivo en sectores específicos, útiles también para hacer frente a esas *ciberinjerencias*[26].

En el ámbito de la seguridad y la defensa, la "Brújula Estratégica", aprobada en marzo de 2022, se convertía igualmente en un importante refuerzo en la lucha contra la *ciberinjerencias*; de hecho, una de las grandes áreas en las que este nuevo instrumento pretende trabajar es el impulso y desarrollo de la *ciberdiplomacia*, en particular con medidas dirigidas a luchar contra la manipulación de la información y la injerencia extranjera[27]. A tal fin, se propone ampliar la denominada *EU Hybrid Toolbox*, para ofrecer una respuesta coordinada frente a cualquier campaña híbrida que afecte a la Unión y sus Estados miembros. Otras iniciativas son los equipos de respuesta rápida híbrida (*EU Hybrid Rapid Response Teams*, que actuaron por primera vez en Ucrania[28]), un Centro de Coordinación del Dominio Cibernético y de la Información (*Cyber and Information Domain Coordination Centre*)[29], así como un mecanismo conjunto operacional que permita supervisar los procesos electorales.

Con independencia de las iniciativas anteriormente mencionadas, el Parlamento Europeo (como he apuntado) se propuso abordar la cuestión de las injerencias en procesos electorales de una manera más concreta. El resultado fue la ya citada resolución de 9 de marzo de 2022, sobre injerencias extranjeras en todos los procesos democráticos de la UE, incluida la desinformación, que considera que la protección de los mismos debería ser "cuestión prioritaria de seguridad nacional", porque es precisamente en este contexto

---

por el que empresas y sociedades aceptaban un conjunto de reglas voluntarias (al respecto, MAURICE, E., "European democracy, a fundamental system to be protected", *European Issues*, Fondation Robert Schuman, Policy Paper nº 578, diciembre 2020). El 16 de junio de 2022 se presentaba una versión mejorada de ese Código (*https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation*).

[25] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea, COM(2020) 790 final, 3 de diciembre de 2020. El Plan proponía medidas legales concretas sobre la publicidad política, que aclararán las responsabilidades de patrocinadores de contenidos de pago, de los canales de producción y distribución y de las consultoras políticas, *https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250*

[26] Reglamento (UE) núm. 2022/2065, de 19 de octubre, del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE, DOUE L 277, de 27 de octubre de 2022; la conocida como Directiva NIS 2 o Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (DOUE L 333, de 27 de diciembre de 2022) y Directiva (UE) 2022/2557, del Parlamento Europeo y del Consejo, de 14 de diciembre, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE (DOUE L 333, de 27 de diciembre de 2022). Todas forman parte de lo que se ha denominado "sistema de ciberdefensa activa y pasiva"·(BERMEJO GARCÍA, R. y LÓPEZ-JACOÍSTE DÍAZ, E., *La ciberseguridad a la luz del jus ad bellum y del jus in bello*, Eunsa, Pamplona, 2020, p. 28).

[27] Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales, doc. 7371/22, Consejo de la Unión Europea, 21 de marzo de 2022, p. 3.

[28] Para controlar posibles ciberataques en estructuras críticas, básicamente (BBC, 22 de febrero de 2022).

[29] Sobre el que existe aún poca información: *https://www.pesco.europa.eu/wp-content/uploads/2022/10/Flyer-CIDCC-221004.pdf*


DOI: 10.17103/reei.45.03

"donde la injerencia extranjera se vuelve más peligrosa"[30]. El Consejo, en sus "Conclusiones sobre un Marco para una respuesta coordinada de la Unión a campañas híbridas" (21 de junio de 2022), invitó al Alto Representante y a la Comisión a "desarrollar opciones de medidas bien definidas que podrían tomarse contra actores FIMI [*Foreign Information Manipulation and Interference*] cuando sea necesario para proteger el orden público y la seguridad en la UE"[31].

Aunque los próximos meses se espera que las acciones concretas de la Unión se materialicen en algo más (una propuesta de la Comisión sería lo deseable), puede decirse que existe ya un convencimiento generalizado de la necesidad de que comiencen cuanto antes a desarrollarse.

## III. ¿ESTAMOS ANTE UN HECHO ILÍCITO A LA LUZ DEL DERECHO INTERNACIONAL DE LA RESPONSABILIDAD?

Para el Parlamento Europeo, las *ciberinjerencias* en procesos democráticos, además de constituir una "grave violación de los valores y principios universales en los que se fundamenta la Unión (…)", son una estrategia de guerra híbrida, "una violación del Derecho internacional" y "una grave amenaza para la seguridad y la soberanía de la Unión"[32].

Como ya se advirtió, este análisis se centrará en las ciberinjerencias como amenazas a la soberanía estatal. El Parlamento parte de la premisa de que son violaciones del Derecho Internacional, con lo que procede primero aclarar algunas dudas respecto de las normas aplicables: ¿cuándo existe esa violación?, ¿qué respuestas podría activar por parte de los Estados afectados?, ¿ha optado la Unión por alinearse con lo que dicte el Derecho Internacional en esta cuestión o también está abierta a promover un mecanismo de reacción propio, más concreto y definido? A dar respuesta a todo lo anterior, o al menos intentarlo, se dedican los dos apartados siguientes.

### 1. Según el Derecho Internacional

Una *ciberinjerencia* en procesos democráticos sería un hecho ilícito internacional en tanto en cuanto fuera susceptible de contravenir el principio de soberanía y la obligación de no intervención. Dado que esas acciones transcurren en el ciberespacio, la cuestión realmente problemática implica determinar si en todos los casos es así y si todos los Estados, o al menos una amplia mayoría de ellos, estarían de acuerdo en esa apreciación. Veámoslo.

[30] Párrs 83 y BC, respectivamente, de la resolución.
[31] Council Conlusions on a Framework for a coordinated EU response to hybrid campaigns, Press Release 603/22, 21 de junio de 2022, párr. 14. Véase también Council Conclusions on FIMI, 18 de julio de 2022, doc. 11429/22, párr. 6.
[32] Párrs. A y E de la resolución de 9 de marzo de 2022, *óp. cit.*, nota 10.


DOI: 10.17103/reei.45.03

### A) ¿UNA VIOLACIÓN DE LA SOBERANÍA? REINO UNIDO, EL VERSO SUELTO

Soberanía y no intervención son conceptos conectados estrechamente: difícil entender el uno sin el otro, aunque encierren elementos diferentes. Con todo, el concepto de soberanía es más amplio que el de no intervención, en tanto en cuanto es el poder del Estado para comportarse según su voluntad y sin más restricciones que las que libremente acepte y/o las impuestas por el Derecho Internacional.

El principio de soberanía, al menos en su versión más tradicional, parece vincularse a acciones contra la integridad territorial de un Estado[33], y esa ha sido precisamente la razón por la cual trasladarlo al ciberespacio ha resultado polémico. Aunque el Manual de Tallín 2.0 sobre la aplicación del Derecho Internacional al Ciberespacio tuvo clara su aplicación en este ámbito (su norma 1 establece que el principio de soberanía se aplica al ciberespacio y la norma 4 afirma que un Estado no debe llevar a cabo *ciberoperaciones* que violen la soberanía de otro)[34], hubo cierta división de opiniones en el Grupo de Expertos que se encargó de su redacción: no surgieron fisuras al determinar que una violación de la soberanía normalmente exige que la operación en el ciberespacio se produzca o se manifieste en la infraestructura cibernética en el territorio del Estado afectado, pero sí al querer reconocer que la soberanía también podría estar bajo amenaza cuando exista una injerencia o usurpación de una función intergubernamental c*on independencia de dónde tenga lugar* la *ciberoperación*[35]. La mayoría terminó aceptándolo, pero algunos Estados siguieron insistiendo en la necesidad de vincularla a la territorialidad[36].

---

[33] Así se aprecia en el asunto Isla de las Palmas (Holanda, Estados Unidos), 4 de abril de 1928, *Report of International Arbitral Awards,* vol. II, pp. 829-871, p. 838: "La soberanía en las relaciones entre Estados significa independencia. La independencia respecto a una porción del globo es el derecho a ejercer en ella, con exclusión de cualquier otro Estado, las funciones propias de un Estado". El principio fue evolucionando, para considerarse también como "la negación de toda subordinación jurídica a una voluntad exterior a la del Estado" (CARRILLO SALCEDO, J. A., "Droit international et souveraineté des Etats. Cours général de droit international public", *RCADI*, vol. 257, 1996, pp. 35-222, p. 60).

[34] *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, en SCHMITT, M. (ed.), Cambridge University Press, Cambridge, 2017, pp. 11 y 17, respectivamente. Aunque no vinculante, se considera ya una obra de referencia en cuestiones sobre el ciberespacio. Sobre cómo surge y los primeros resultados, GUTIÉRREZ ESPADA, C., "¿Existe (ya) un derecho aplicable a las actividades en el ciberespacio?", en CERVELL HORTAL, M. J. (dir.), *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio,* Aranzadi, Cizur Menor, 2020, pp. 225- 248, pp. 237-238. Sobre distintas posturas doctrinales acerca de la aplicación del principio, MOYNIHAN, H., "The vital role of International Law in the framework for responsible State behaviour in cyberspace", *Journal of Cyber Policy,* vol. 6, 3, 2021, https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550, pp. 394-410, p. 400. Véase también el Informe que sirvió de base para elaborar la Declaración italiana sobre el ciberespacio: "International Law and cyberspace", Report of the Study Group co-organised by the University of Bologna, University of Milan and University of Westminster, February 2021, pp. 3-4, https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf

[35] *Tallinn Manual 2.0..., óp. cit.* nota 34, p. 23, párr. 19.

[36] *Íd.*, párr. 20.


DOI: 10.17103/reei.45.03

También sobre la cuestión se pronunciaron los grupos que, en el seno de Naciones Unidas, estudian la cuestión del ciberespacio[37]. Tanto el Grupo de Trabajo de Composición Abierta (liderado por Rusia)[38] como el Grupo de Expertos Gubernamentales sobre el fomento del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional[39] fueron partidarios de la opción más cauta, limitándose a vincular la soberanía con la jurisdicción sobre las infraestructuras de su territorio .

En el supuesto de injerencia en elecciones electorales, parece claro que existiría una violación de soberanía cuando se tratara de una *ciberoperación* que produjera daños físicos sobre una infraestructura directamente vinculada a un proceso democrático situada en un Estado (sistema informático de recuento de voto, terminales de voto electrónico…), pero mayores interrogantes plantearían otros supuestos, como difundir información falsa sobre los candidatos para intentar cambiar la intención de voto[40], en los que ese vínculo territorial ya no sería tan claro. En todo caso, parece que movernos en el ciberespacio obligaría a ciertos cambios en el planteamiento hasta ahora más tradicional (como hizo la mayoría del Grupo de Tallín): ¿cómo no admitir que una *ciberoperación* que limite, condicione o modifique la decisión de un Estado (en este caso, los procesos electorales que en él se celebran) no viola el principio de soberanía (también el de no intervención, como se verá en el apartado siguiente), por más que no haya esa conexión directa con el territorio? En otros tiempos (analógicos) podría ser coherente, pero ya no.

Respecto de lo que opinan los Estados al respecto, una amplia mayoría (cada uno con sus propios matices e interpretaciones) acepta que una *ciberoperación* puede, en general y sin pronunciarse más al respecto, violar el principio de soberanía. Así lo hacen Canadá[41],

[37] El Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional que, entre otras cuestiones, dejó claro en sus informes de 2013 y 2015 (doc. A/68/98 de 24 de junio de 2013 y doc. A/70/174 de 22 de julio de 2015, respectivamente) que el Derecho internacional se aplica al ciberespacio, dividió en 2018 sus trabajos, que fueron asumidos por otros dos grupos de, digámoslo así, sensibilidades diferentes. El Grupo de Trabajo de Composición Abierta (*Open-Ended Group*) sobre la evolución de las TIC en el contexto de la seguridad internacional (doc. A/C.1/73/L.27/Rev.1, 29 de octubre de 2018) fue auspiciado por Rusia y ha sido prorrogado hasta 2025 (A/RES/75/240, 31 de diciembre de 2020). El otro grupo, Grupo de Expertos Gubernamentales sobre el fomento del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, promovido por Estados Unidos, redactó su informe final en mayo de 2021 (doc. A/76/135, 14 de julio de 2021).

[38] A/AC.290/2021/CRP.2, 10 de marzo de 2021, párr. 19.

[39] Informe Final de 28 de mayo de 2021, doc. A/76/135, *óp. cit*., nota 37, párr. 71.

[40] SCHMITT, M., "Foreign cyber interference in elections: an International Law Primer, Part II", *EJIL Talk*, 16 de octubre de 2020.

[41] International Law applicable in cyberspace. Government of Canada, April 2022, párr. 10 *https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng*


DOI: 10.17103/reei.45.03

Brasil[42], China[43] o Italia[44], y también la OTAN comulga con esas opiniones[45], aceptando que *ciberoperaciones* que no traspasen el umbral del uso de la fuerza o del ataque armado violen, en su caso, ese principio. Por su parte, Francia sí parece vincularlo expresamente al territorio ("La France exerce sa souveraineté sur les systèmes d'information situés sur son territoire") [46], mientras que otros se muestran más abiertos a no hacerlo, como Países Bajos[47], Alemania[48] o República Checa[49].

---

[42] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, doc. A/76/136, 13 de julio de 2021, pp. 18-19.

[43] China's Positions on International Rules-making in Cyberspace, 20 de octubre de 2021, párr. II, ii, disponible en *https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html*

[44] Italian Position Paper on International Law and Cyberspace, 2021, disponible en https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf, pp. 4-5.

[45] La OTAN afirma que las *ciberoperaciones* (COs) "that generally would not constitute a use of force or armed attack might involve effects that create only temporary disruptions or denials of service, or those intended merely for disseminating or gathering information" (*Allied joint doctrine for cyberspace operations*, *AJP-3.20*, enero de 2020, p. 20, párr. 3.7 disponible en *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf*), precisando en la nota al pie 26: "Depending on the context, such COs may nevertheless *constitute a violation of international law as a breach of sovereignty* or other internationally wrongful act" (cursiva añadida).

[46] *Droit international appliqué aux opérations dans le cyberespace*, 2019, p. 6, disponible en *https://www.defense.gouv.fr/sites/default/files/ema/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf*

[47] Eso sí, insiste en que esto es aún "cuestión debatida" (*Letter to the Parliament on the International Legal order in cyberspace, Appendix International Law in cyberspace*, 26 de septiembre de 2019, p. 3, disponible en *https://www.thehaguecybernorms.nl/annex-to-the-application-of-international-law-to-cyber-operations*).

[48] On the Application of International Law in Cyberspace. Position Paper, March 2021, p. 3 (*https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf*). Reconoce que, de existir el elemento coercitivo, sería ya una violación del principio de no intervención. Y parece, además, abierta a ir más allá del vínculo territorial: "violations of State sovereignty may inter alia involve its territorial dimension" (obsérvese el uso de "may"). Al respecto, F. KRIENER afirma que defender la violación de la soberanía en estos casos es lo lógico y necesario, pero que también podría tener consecuencias negativas, como restringir "la promoción de la democracia, en la que Alemania participa con frecuencia" ("Cyber space, sovereignty and the intricacies of International Law-making", 16 de abril de 2021, https://voelkerrechtsblog.org/cyber-space-sovereignty-and-the-intricacies-of-international-law-making/). Sobre la declaración alemana, KRIENE, F., "Cyber space sovereignty and the intricacies of International Law Making. Reflections on Germany's position paper on International law in cyberspace", 16 abril de 2021, *https://voelkerrechtsblog.org/cyber-space-sovereignty-and-the-intricacies-of-international-law-making/*

[49] Statement by Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department (check against delivery) at the 2 nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the the General Assembly of the United Nations, p. 3, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf. Enumera incluso casos de *ciberoperaciones* que violarían


DOI: 10.17103/reei.45.03

En contra de esa corriente dominante que acepta sin grandes problemas que determinadas *ciberoperaciones* vulneran el principio de soberanía, se ha manifestado el Reino Unido[50], que prefiere centrarse en la norma que prohíbe la intervención cuando existan *ciberinjerencias*. La razón que aduce es, básicamente, que el principio de soberanía no tiene la consideración de norma primaria del Derecho Internacional[51] y que no aporta más que lo que ya implica el principio de no intervención ¿Es un argumento adecuado y, sobre todo, coherente? ¿Cuáles son sus razones para defenderlo?

En junio de 2021, las opiniones acerca del ciberespacio del Reino Unido y otros catorce Estados quedaron reflejadas en un Anexo del Informe del Grupo de Expertos Gubernamentales que trabaja en Naciones Unidas en esa cuestión, en el que el Reino Unido reiteró que la soberanía no "proporciona una base suficiente o clara para extrapolar una norma específica o una prohibición adicional para la conducta cibernética que vaya más allá de la no intervención"[52]. Idéntico argumento siguió defendiendo la Fiscal General del Estado (*Attorney General*), Suella Braverman, en su discurso ante la *Chatham House* de Londres el 19 de mayo de 2022[53].

Esa es también la postura británica dentro de la OTAN[54], por más que ninguno del resto de miembros, y tampoco la propia Organización, como vimos, la compartan. Para el Reino Unido, en efecto, la mejor base para frenar ciertas acciones en el ciberespacio sigue siendo la prohibición de intervención en asuntos de otros Estados. Mantener esta opinión le permitiría llevar a cabo *ciberoperaciones* en territorio de otro Estado sin cometer un hecho internacionalmente ilícito basado en la violación de la soberanía de dicho Estado,

---

la soberanía y que van más allá del vínculo territorial, aceptando operaciones que manipulen datos o servicios inherentes a las funciones gubernamentales.

[50] Véase el discurso de Jeremy Wright (*Attorney General*) sobre la posición del Reino Unido sobre la aplicación del Derecho Internacional al ciberespacio, publicado el 23 de mayo de 2018 y disponible en https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. También el de su sucesora, Suella Braverman, en 2022, *UK's position on applying international law to cyberspace, Attorney's General Speech Suella Braverman*, Chatham House, 19 de mayo de 2022, *https://www.gov.uk/government/speeches/international-law-in-future-frontiers*. Sobre el contenido de ese discurso y también sobre la posición británica acerca de la aplicación del principio de soberanía al ciberespacio, SCHMITT, M., "The United Kingdom on International Law in cyberspace", *EJIL Talk*, 24 May 2022.

[51] Aunque también son mayoría los autores que lo defienden como norma jurídica, otros alegan lo contrario, argumentando, por ejemplo, que los diferentes regímenes de soberanía que existen en tierra, mar y aire son la mejor prueba de que la existencia de una "norma universal de soberanía" es una "falacia" y que, por tanto, tampoco podría aplicarse al ciberespacio (CORN, G. P. y TAYLOR, R., "Symposium on sovereignty, cyberspace and Tallinn Manual 2.0. Sovereignty in the age of cyber", *AJIL Unbound*, vol 111, 2017, pp. 207-212, p. 210). Esa tesis, en concreto, ha sido puesta en duda por M. SCHMITT y L. VIHUL ("Respect for sovereignty in space", *Texas Law Review*, vol 95, 2017, pp. 1639-1670, p. 1644 y "Sovereignty in cyberspace: lex lata vel non?", *AJIL Unbound*, vol 111, 2017, pp. 213-218).

[52] Official compendium*…, óp. cit*., nota 42, párr. 10.

[53] *Attorney's General Speech Suella Braverman*, *óp. cit*., nota 50.

[54] Así lo afirmaba al comentar el documento *NATO Standard AJP-3.20. Allied Joint Doctrine for cyberspace operations, óp. cit.*, nota 45: "The AJP refers to cyberspace operations as being, dependent on the context, potential violations of international law as a breach of sovereignty. Whilst sovereignty is fundamental to the international rules-based system, the UK government does not consider that the current state of international law allows for a specific rule or additional prohibition for cyberspace operations beyond that of a prohibited intervention".


DOI: 10.17103/reei.45.03

pero también tendría que asumir que operaciones de otros Estados dirigidas contra él no podrían ser consideradas una violación de su propia soberanía[55]. Por otro lado, aceptar que una *ciberoperación* viola también el principio de soberanía conlleva la ventaja de que no se exige en este caso el elemento coercitivo, presente en el de no intervención, lo que abre claramente el ámbito de aplicación (*vid infra*, apartado siguiente), pero también es cierto que el Reino Unido parte de un concepto amplio de ese elemento, que le permitiría aceptar como violaciones del Derecho internacional un abanico más amplio de acciones[56].

Sea como fuere, hay quien vaticina que acaso la cuestión ya no sea tan importante ni que haya que interpretar estrictamente la postura británica: cada vez es mayor el número de Estados que admite expresamente que una *ciberoperación* puede violentar el principio de soberanía y al Reino Unido no le interesa aferrarse a un debate vacuo si quiere encontrar opciones y aliados para moverse en "terreno común" a la hora de calificar como ilegales las operaciones cibernéticas[57].

### B) TAMBIÉN UNA VIOLACIÓN DEL PRINCIPIO DE NO INTERVENCIÓN

El principio de no intervención, expresión máxima de la soberanía estatal, es una norma consolidada en Derecho Internacional, cuya naturaleza consuetudinaria ha sido confirmada, sabido es, por la Corte Internacional de Justicia (CIJ)[58]. Por su parte, la "Declaración sobre inadmisibilidad de la intervención en los asuntos internos de los Estados y protección de su independencia y soberanía" de la resolución 2131 (XX), de 21 de diciembre de 1965 (que contó con la única abstención de Reino Unido), consagra una *tesis amplia* sobre la prohibición, que prohíbe expresamente "cualquier otra forma de injerencia o de amenaza atentatoria de la personalidad del Estado, o de los *elementos políticos*, económicos y culturales que lo constituyen" (párr. 2, cursiva añadida). También la resolución 2625 (XXV) de 1970 de la Asamblea General de las Naciones Unidas considera contraria al principio toda medida que atente contra la personalidad de un Estado o sus elementos políticos, sociales, económicos o culturales. Algunos años después, la "Declaración sobre la inadmisibilidad de la intervención y la injerencia en los asuntos internos de los Estados" (resolución 36/103, de 9 de diciembre de 1981) ampliaría la norma, al declarar expresamente el deber de los Estados de "abstenerse*"* de todo acto

[55] De hecho, como algún autor ha apuntado, el aceptar o no que una *ciberoperación* viola el principio de soberanía ha llevado a ciertas contradicciones en los Estados que critican o condenan conductas de otros (para ejemplos concretos, KENNY, J., "France, cyber operations and sovereignty: the purist approach to sovereignty and contradictory State practice", *Lawfare*, 12 de marzo de 2021, https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice).

[56] *Attorney's General Speech Suella Braverman*, *UK's position on applying international law to cyberspace*, *óp. cit.*, nota 50.

[57] SCHMITT, M., *óp. cit*., nota 50.

[58] Asunto sobre las actividades militares y paramilitares en y contra Nicaragua, sentencia de 27 de junio de 1986, *ICJ Reports 1986*, p. 106, párr. 202 y asunto relativo a las actividades armadas en territorio del Congo (República Democrática del Congo c. Uganda), sentencia de 19 de diciembre de 2005, *ICJ Reports 2005*, p. 227, párrs. 162-164.


DOI: 10.17103/reei.45.03

de injerencia "política" (también militar y económica)[59]. Resoluciones posteriores de la Asamblea General siguieron defendiendo la no injerencia, ya con referencias expresas a los procesos electorales[60].

La intervención en un proceso democrático supondría, en definitiva, una injerencia en los elementos políticos de un Estado y, por tanto, una violación del principio de no intervención. ¿Es trasladable esta afirmación al ciberespacio? La regla 66 del Manual de Tallín 2.0[61] lo admite y en esa misma línea se pronunciaba el Grupo de Expertos Gubernamentales de Naciones Unidas en sus Informes de 2015 y 2021[62]. Sin embargo, el informe final del Grupo de Trabajo de Composición abierta (recordemos, el liderado por Rusia), no se mostraba tan abiertamente partidario al respecto y, de hecho, en su Informe final de marzo de 2021 omitía mención alguna al principio de no intervención.

Parece, por tanto, que con la salvedad de algunos Estados (a algunos de los cuales se aludirá más tarde) existe cierto consenso, aunque más discutido por algunos (Rusia a la cabeza), de que ciertas actividades en el ciberespacio pueden violar el principio de no intervención.

En noviembre de 2022, el Primer Comité de la Asamblea General adoptó una resolución, liderada por Francia, incluyendo un Programa de Acción sobre avances en el comportamiento estatal responsable en el ciberespacio[63], que se activará una vez que el Grupo de Trabajo de Composición Abierta termine sus trabajos en 2025 y que pretende buscar soluciones comunes (dejando, pues, atrás las dos líneas de trabajo existentes hasta ahora). Si habrá pronunciamiento expreso sobre la no intervención es algo que está aún por ver. Mientras tanto, la duda que persiste es si, aun aceptando que el principio de intervención es aplicable al ciberespacio, debería introducirse algún tipo de matiz. O dicho de otro modo, ¿todos sus elementos deben trasladarse de manera idéntica cuando el entorno en el que se produce es diferente? Más en concreto, y centrándonos en el objeto de este trabajo, cuando determinados procesos electorales se vean afectados por injerencias externas fruto de actividades cibernéticas, ¿podríamos hablar de violaciones del principio de no intervención?

Si en el pasado cuestiones como la financiación de partidos por Estados terceros, el apoyo activo a ciertas opciones políticas u otro tipo de intervenciones dirigidas a dar un vuelco a unas elecciones fueron los principales problemas relacionados con la manipulación de

[59] Al respecto, OSSOF, W., "Hacking the domaine réservé: the rule of non-intervention and political interference in cyberspace", *Harvard International Law Journal*, vol. 62, 1, 2021, pp. 296-323, p. 302.
[60] *Ad. ex*. A/RES/48/124, de 14 de febrero de 1994, párr. 3 y A/RES/56/154, de 19 de diciembre de 2001, párr. 4.
[61] *Tallinn Manual 2.0…óp. cit.*, nota 34, norma 66, p. 312. Al respecto, GUTIÉRREZ ESPADA, C., *De la legítima defensa en el ciberespacio*, Comares, Granada, 2020, pp. 33-36.
[62] Doc. A/70/174, *óp. cit*., nota 37, párr. 28, b) y doc. A/76/135, de 14 de julio de 2021, *óp. cit*., nota 37, párr. 71.
[63] Con 157 a votos y 6 en contra (China, República Democrática de Corea, Irán, Nicaragua, Rusia y Siria). El Programa de Acción puede consultarse en el doc. A/C.1/77/L.73, 13 de octubre de 2022.


DOI: 10.17103/reei.45.03

procesos electorales[64], el ciberespacio obliga a afrontar estas y otras acciones bajo una óptica distinta. Lo cierto es que, desde que la CIJ se pronunciara sobre el principio en el asunto Nicaragua, pocos avances relevantes más ha habido respecto de su naturaleza y conformación[65] pero, ¿y si el ciberespacio obliga a modificar algunas de sus características hasta ahora consolidadas? Tradicionalmente, para conculcar el principio, se han exigido, recordemos, dos elementos, respaldados por la CIJ:

- La intervención debe afectar a los asuntos propios de un Estado, ya sean externos o internos; esto es, debe recaer en lo que se conoce como su espacio de soberanía (*domaine réservé*)[66].
- Y debe, además, darse un elemento coercitivo, requisito que fue calificado por la Corte como "la esencia fundamental"[67], pero que no definió con precisión. La letra de la resolución 2625 de la Asamblea General parece sugerir que se trata de no forzar que el Estado tome decisiones que de otro modo no hubiera tomado. También el Grupo de Tallín aceptó este elemento[68].

*A priori*, todo proceso electoral formaría parte de ese *domaine reservé* (de hecho, la CIJ citó expresamente "elección del sistema político" en la sentencia Nicaragua)[69], con lo que la presencia del primer elemento no encontraría grandes dificultades, pero cuando se traslada al ciberespacio surgen más dudas, porque en él resulta demasiado limitado[70] y abstracto[71]. Por eso hay quien propone el cambio a "*domaine privilégié*"; es decir, ámbitos

[64] Sobre estas modalidades, digamos, tradicionales, puede consultarse FISLER DAMROSH, L., "Politics across borders: non intervention and nonforcible influence over domestic affairs", *AJIL*, vol 83, 1, 1989, pp. 1-50 (pp. 13-34).

[65] POMSON, O., "The Prohibition on Intervention Under International Law and Cyber Operations", *International Law Studies*, vol 99, 2022, pp. 180-219, p. 211.

[66] Asunto sobre las actividades militares y paramilitares en y contra Nicaragua, *óp. cit.*, nota 58, p. 108, párr. 205. Previamente, el Instituto de Derecho Internacional se había referido al concepto como "celui des activités étatiques où la compétence de l'Etat n'est pas liée par le droit international" (art 1, resolución "La determination du domaine rérservé et ses effets", sesión de Aix-en-Provence, 1954). Sobre el concepto *domaine réservé*, ARANGIO RUIZ, G., "Le domaine réservé: l'organisation international et le rapport entre droit international et droit interne", *RCADI*, vol. 225, 1990, VI, pp. 9-48 (pp. 428-434).

[67] *Íd*. En realidad, este concepto fue ya usado por la Corte Permanente de Justicia Internacional en la Opinión consultiva sobre documentos de nacionalidad expedidos en Túnez y Marruecos, *PCIJ Series B*, nº 4, 7 de febrero de 1923, pp. 23-24. Sobre este concepto (y también el anterior), POMSON, O., *óp. cit*., nota 65, pp. 182-183.

[68] *Tallinn Manual*, *óp. cit*., nota 34, p. 319. Sobre estos elementos, HELAL, M. S., "On coercion in International Law", *Public Law and Legal Theory Working Paper Series No. 475*, March 21, 2019, pp. 2-82, pp. 65 y ss. y pp. 70-76, en *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3357513*. También sobre esos elementos, MOULIN, T., "Reviving the principle of non-intervention in cyberspace: the path forward", *Journal of Conflict and Security Law*, vol. 25, 3, 2020, pp. 423-447 (pp. 430-433 y 443-446) y OHLIN, J. D., "Did Russian cyber interference in the 2016 elections violate International Law?", *Texas Law Review*, vol. 95, 2017, pp. 1579-1598 (pp. 1587-1593).

[69] Asunto sobre las actividades militares y paramilitares en y contra Nicaragua, *óp. cit.*, nota 58, p. 108, párr. 205.

[70] HOLLIS, D., "The influence of war; the war for influence", *Temple International Law and Comparative Law Journal*, vol. 32, 1, 2018, pp. 31-46, p. 40.

[71] Véase OHLIN, J. D., "Did Russian…", *óp. cit.*, nota 68, pp. 1587-1588. También MOYNIHAN, H., "The application of International Law to State cyberattacks", *Chatham House Research Paper*, 2019, p. 34. En la misma línea, OSSOF, W., *óp. cit.*, nota 59, p. 307.


DOI: 10.17103/reei.45.03

quizás no necesarios para la supervivencia de un Estado pero sí para "su independencia, autonomía y estabilidad", como pudiera ser la organización política del Estado, la seguridad exterior, los intereses económicos, los servicios públicos (salud y otros), el medio ambiente…[72].

También plantea problemas el segundo elemento, el coercitivo, sobre todo porque la injerencia en procesos democráticos, en ocasiones, no es tanto coerción (presión real para forzar a ese Gobierno a hacer algo o, incluso, privarle del control en la toma de decisiones) cuanto *intención* de persuadir o influenciar[73]. En efecto, respecto de procesos democráticos o de toma de decisiones, podría hablarse de dos tipos de acciones:

- *Ciberinjerencias* "materiales", en las que un tercer Estado se entromete en cuestiones que deberían ser directamente llevadas a cabo por las autoridades estatales a las que se encarga la gestión de unas elecciones o que afectan a la propia infraestructura electoral. El ejemplo obvio sería el uso de medios cibernéticos para provocar un recuento erróneo (manipulando directamente los resultados, inutilizando o manipulando la maquinaria electoral, bloqueando el voto electrónico, etc…), o la difusión de información falsa (de importancia, a gran escala y que resulte convincente) sobre cómo y/o dónde emitir el voto o impedirlo físicamente de una manera concreta (por ejemplo, amenazando con hacer estallar un artefacto en los colegios electorales[74]).
- *Ciberinjerencias* "inmateriales", que pretenden más bien cambiar la actitud de los votantes hacia un partido o representante. Por ejemplo, impedir que una parte importante del electorado tenga acceso a la información de todos los candidatos o manipular reiteradamente los datos sobre los mismos (cuando se *hackean* de manera masiva o continuada sus páginas web o determinados medios de comunicación atacan o defienden claramente a unos u otros, o cuando se usa la inteligencia artificial para crear perfiles falsos, generar rumores negativos o atribuir delitos a esos candidatos...). En estos casos concretos, la presencia del elemento coercitivo no siempre es clara porque en la mayoría de estos supuestos se pretende hacer circular cierta información para que un candidato sea visto con mejores (o peores) ojos. Serían más bien campañas de *propaganda* que, en principio, no llevarían aparejada coerción alguna, pero, ¿y si, al calor de las facilidades de difusión que ofrecen las redes, fueran realmente capaces de cambiar una elección u otro proceso decisorio y, además, hubieran sido orquestadas a tal fin por un Gobierno? El panorama sería ya distinto y lo lógico sería aplicar a cada caso un criterio de *cantidad* o *umbral* mínimo: si la influencia que se ha ejercido es de tal magnitud que el proceso ha dado un vuelco

[72] MOULIN, T., *óp. cit.*, nota 68, pp. 425 y 433-438.
[73] Véase al respecto OHLIN, J. D., "Election interference: the real harm and the real solution", *Legal Studies Research Paper*, Cornell Law School, disponible en *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3276940*. El autor realiza también una interesante conexión entre la injerencia en elecciones y el principio de libre determinación de los pueblos. También conectando los dos conceptos, TSAGOURIAS, N., "Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace", *EJIL Talk*, 26 August 2019.
[74] SCHMITT, M. "Foreign cyber interference in elections: an International Law Primer, Part I", *EJIL Talk*, 16 de octubre de 2020.


DOI: 10.17103/reei.45.03

> claro, sí debería reconocerse que la acción ha sido coercitiva[75] (el Estado habría perdido el *control*) y concluir, por tanto, que estamos ante una violación del principio de no intervención. Fijar la línea divisoria, eso sí, no es sencillo[76].

Ciertamente, una concepción restrictiva del elemento coercitivo, centrada sólo en injerencias de las que hemos calificado como "materiales", limitaría el campo de acción y reacción de los Estados. La cuestión es ciertamente compleja, porque antes de que el ciberespacio irrumpiera, ya se apuntó, el hecho de influir, manipular de manera limitada, hacer campaña o promoción a favor de ciertas líneas políticas era algo, digámoslo así, aceptado en las relaciones internacionales, pero las herramientas que ofrece el ciberespacio han provocado que esas acciones crezcan en magnitud, gravedad y consecuencias.

Lo cierto es que ya hay Estados que se muestran receptivos a incluir conductas que supongan manipulación de elecciones o de intención de voto, pero aunque algún autor hable de una nueva costumbre que podría estar cristalizando y cambiar así algunas de las características del principio de no intervención[77], su número es todavía reducido y, dentro de ellos, son menos aún los que se abren a considerar de manera expresa que las *cibereinjerencias* inmateriales también estarían prohibidas. En efecto, a la luz de las declaraciones formales de los Estados, y sin ánimos de ser exhaustivos, podríamos diferenciar varias líneas de posicionamiento:

a) En primer lugar, Estados que consideran que las *ciberinjerencias* en procesos electorales violan el principio de no intervención, pero que (sólo) *aparentemente* se centran en *ciberinjerencias* materiales. Estados Unidos, por ejemplo, considera que "una operación cibernética de un Estado que interfiera en la capacidad de otro para celebrar unas elecciones o que manipule los resultados electorales de otro país sería una clara violación de la norma de no intervención"[78] y algo similar declara Australia[79].

---

[75] De "escala" y "efectos" habla M. SCHMITT: hasta qué punto se han visto afectadas las elecciones, si se trataba de elecciones municipales o nacionales, ... (*óp. cit*, nota anterior).

[76] Ya hay opiniones contrapuestas. Algún autor afirma, respecto de las acciones rusas en las elecciones estadounidenses de 2016, que hay "substantial impediments" para concluir que fueran ilegales (OHLIN, J. D., "Did Russian …", *óp. cit.*, nota 68, p. 1592). No todos comulgan con esta afirmación; en el otro extremo véase, por ejemplo, BARELA, S. J., "Cross-border cyber operations to erode legitimacy: an act of coercion", *Just Security*, 12 enero de 2017, disponible en *https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/* y TERRY, P., "Don't do as I do- The US Response to Russian and Chinese cyber espionaje and Public International Law, *German Law Journal*, vol. 19, 2018, pp. 614-626, p. 623. Más cautos se muestran otros autores; *ad. ex*. CORTÉS MARTÍN, J. M., "Ciberataques y responsabilidad: sobre las asimétricas incertidumbres del Derecho Internacional vigente", en MILLÁN MORO, L. (dir.) y FERNÁNDEZ ARRIBAS, G. (ed.), *Ciberataques y ciberseguridad en la escena internacional*, Aranzadi, Cizur Menor, 2019, pp. 51-70, p. 58: "es difícil concluir con rotundidad que ese tipo de campañas podrían ser intervenciones coercitivas".

[77] POMSON, O., *óp. cit.*, nota 65, pp. 183-184 y 217-218.

[78] Official compendium …, *óp. cit.*, nota 42, p. 140.

[79] Anexo B (*Australia's position on how international law applies to State conduct in cyberspace*): "…the use by a hostile State of cyber activities to manipulate the electoral system to alter the results of an election in another State, (…) would constitute a violation of the principle of non-intervention" (*https://www.internationalcybertech.gov.au/our-work*).


DOI: 10.17103/reei.45.03

Aunque en ambos casos pudiera pensarse que las referencias van, en efecto, más enfocadas a manipulaciones materiales (recuento de votos, impedir ejercer el derecho…), la amplitud de los términos que emplean ("interferir en la capacidad […] para celebrar elecciones", manipulación de resultados o del sistema electoral…) permitiría incluir ciertas *ciberinjerencias* inmateriales, al menos aquellas en las que el elemento coercitivo fuera más claro.

Nueva Zelanda también admite que ciertas *cibermanipulaciones* en procesos electorales pueden violar el principio, ofreciendo como ejemplos específicos la manipulación del recuento final de votos o impedir que parte significativa de la población ejercite su derecho a votar[80].

Esa aparente preferencia por las *ciberinjerencias* materiales se observa también en la Declaración de Canadá, que se refiere expresamente a acciones cibernéticas que "pirateen e inutilicen la comisión electoral de un Estado días antes de unas elecciones" y que proclama que "la práctica de los Estados y la *opinio* iuris ayudarán a aclarar, con el tiempo, los umbrales de la norma de no intervención y el alcance del derecho consuetudinario en este ámbito"[81].

b) En segundo lugar podríamos referirnos a Estados que abiertamente admiten que la mera manipulación del electorado podría ser suficiente para considerar violado el principio de no intervención. Sorprende, por ejemplo, por su amplitud, la Declaración de Irán sobre el Derecho Internacional aplicable al ciberespacio, en la que se afirma expresamente lo siguiente:

> "Medidas como la manipulación cibernética de las elecciones o la ingeniería de la opinión pública en vísperas de las elecciones pueden constituir ejemplos de intervención flagrante. (…) Las actividades cibernéticas que paralizan los sitios web de un Estado para provocar tensiones y conflictos internos o el envío de mensajes masivos de forma generalizada a los votantes para afectar al resultado de las elecciones en otros Estados también se consideran intervenciones prohibidas"[82].

El Reino Unido que, como vimos, considera la no intervención como la norma de referencia en el ciberespacio, contempla expresamente supuestos de *ciberinjerencia* material[83], pero también deja margen a una interpretación más abierta, al declarar que "las "ciberoperaciones encubiertas de un Estado extranjero que interfieran coercitivamente en

[80] The Application of International Law to State Activity in Cyberspace, New Zealand, 1 de diciembre de 2020, párr. 10, *https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf*

[81] International Law applicable in cyberspace. Government of Canada, *óp. cit*., nota 41, párrs. 24 y 25.

[82] Declaración del Estado Mayor de las Fuerzas Armadas de la República Islámica de Irán sobre el derecho internacional aplicable al ciberespacio, agosto de 2020, *https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat*

[83] Operaciones que afecten a sistemas que controlan los recuentos electorales para cambiar el resultado de una elección o que provoquen un mal funcionamiento del sistema de registro de votantes, *Attorney's General Speech Suella Braverman*, *óp. cit*., nota 50.


DOI: 10.17103/reei.45.03

procesos electorales libres y justos constituirían una intervención prohibida"[84]. De hecho, apostilla: "la coerción puede ser más amplia de lo que es"[85].

Amplia es también la postura sobre el ciberespacio de Alemania, que considera que las actividades cibernéticas malintencionadas dirigidas a elecciones extranjeras pueden constituir una intervención ilícita[86]. Admite, además, expresamente, que esa *ciberinjerencia* electoral puede ser tanto material (inutilización de la infraestructura y de la tecnología electoral, como las papeletas electrónicas, etc…,) como inmaterial (por ejemplo, incitar a través de internet a la agitación política violenta, a los disturbios y/o a la lucha civil en un país extranjero, impidiendo así de manera significativa el desarrollo ordenado de unas elecciones y la emisión de los votos). Consciente de que es difícil abarcar todas las posibles conductas, afirma que "sería necesaria una evaluación detallada de cada caso".

c) En tercer lugar podríamos incluir los Estados que se limitan a señalar que el principio de no intervención puede resultar violado si de alguna manera se interfiere en elecciones o en el sistema político, sin entrar en mayores detalles[87].

Son aún, en definitiva, minoría los Estados que han recogido formalmente la *ciberinjerencia* en procesos democráticos como conducta contraria al Derecho Internacional (España aún no se ha pronunciado expresamente ni en este ni en otros temas del ciberespacio y Rusia y China, por ejemplo, no van más allá de una lacónica fórmula en el sentido de que los principios de Derecho Internacional se aplican al ciberespacio)[88].

Es pronto, pues, para poder hablar de una norma consolidada sobre la prohibición del principio de no intervención en el ciberespacio que incluya de manera expresa las *ciberinjerencias* en procesos democráticos y, sobre todo, que admita expresamente las inmateriales, pero también es cierto que ya hay Estados dispuestos a hacerlo. El ciberespacio está abriendo escenarios difícilmente imaginables hace unos años y que terminarán afectando a lo que hasta ahora se ha considerado como *domaine reservé* y coerción. Y valga como muestra un botón: el 2 de mayo de 2022, varios medios de

[84] *Íd*. Es cierto que luego matiza, afirmando que habría que ver caso por caso, pero la formulación abierta de esas "operaciones encubiertas" podría hacer que bajo determinadas consecuencias se considerara como intervención ciertas campañas de manipulación o desinformación electoral de carácter masivo.
[85] *Íd*: "… I want to be clear today that coercion can be broader than this. (…)".
[86] On the Application of …, *óp. cit.*, nota 48, p. 3.
[87] Véase por ejemplo, Brasil: "dado que las elecciones son el núcleo de los asuntos internos de un Estado, si el uso malintencionado de las TIC contra un Estado implica algún nivel de coerción, entonces debe estar prohibido por el principio de no intervención*", Official compendium…, óp. cit*., nota 42, pp. 18-19. También Francia: "la injerencia a través de un medio digital en los asuntos internos o externos de Francia (…), puede constituir una violación del principio de no intervención", *Droit international appliqué …, óp. cit.* nota 46, p. 7.
[88] Rusia y China son firmes defensoras del principio de no intervención y se posicionan en contra de las campañas de propaganda. Ahora bien, defienden una visión particular de la soberanía y el ciberespacio, argumentando que los gobiernos tienen la jurisdicción exclusiva sobre el ciberespacio nacional (las posiciones occidentales, como es sabido, defienden mayor libertad en el ciberespacio). Véase KATAGIRI, N., "Why international law and norms do little in preventing non-state cyber attacks", *Journal of Cybersecurity*, vol. 7, 1, 2021, pp. 1-9, p. 8, doi: 10.1093/cybsec/tyab009.


DOI: 10.17103/reei.45.03

comunicación informaron de que parte de la conexión ucraniana a Internet en la región ucraniana ocupada de Jersón se interrumpió casi por completo, para volver a instalarse horas después. El jefe del Servicio Estatal de Comunicaciones Especiales y Protección de la Información de Ucrania afirmó que las actividades de desvío tenían su origen en Rusia y que constituían una violación del Derecho Internacional, ya que, aunque el desvío fue temporal, en ese tiempo el tráfico de Internet estuvo sometido a las limitaciones que sobre él establece Rusia (censura, prohibición de ciertas plataformas o sitios web...)[89]. Una situación similar podría, dado el caso, darse también en relación con un proceso electoral. ¿podría el desvío de tráfico de internet de un Estado a otro considerarse un acto que interfiere en el *domaine reservé*? ¿Hasta qué punto y/o en qué casos existe un verdadero elemento coercitivo en ese caso?[90]

Con independencia de las etiquetas y denominaciones que queramos acuñar (*ciberinjerencias materiales*, *inmateriales*…), en el ámbito de la intervención en procesos electorales habrá que ser especialmente cuidadoso con las acciones que tienden más bien a influir en la opinión de algunos ciudadanos con informaciones falsas o maliciosas y que, *a priori*, no tendría por qué violar el principio de no intervención, salvo que sean de entidad suficiente. Es difícil, con todo, fijar un umbral y quizás todo pase por, como ya expresamente apunta algún Estado (Canadá, Alemania), solucionar la cuestión analizando el supuesto concreto. Es esa también, como veremos, la línea que parece preferir el Parlamento Europeo. Y puede que incluso algún día nos encontremos con apoyo jurisprudencial que, caso a caso, como en otros ámbitos ha ocurrido (agresión, por ejemplo) nos ilumine el camino, pero acaso también podrían barajarse (a nivel más reducido) otras opciones (*vid infra* apartado III).

## 2. Según la UE: ¿en busca de una definición?

Pese a los intentos que la Unión Europea está haciendo en los últimos años por dotar al entorno ciberespacial de cierto orden y control normativo, no existe definición formal de qué entender por *ciberinjerencia* más allá de la que pudiera deducirse de la expresa aceptación del Derecho Internacional que sobre esta cuestión hace la resolución del Parlamento Europeo de 9 de marzo de 2022 a la que ya varias veces se ha aludido. La remisión, ciertamente, ayuda poco, pues como se ha podido advertir en los apartados anteriores, el concepto de *ciberinjerencia* y cuándo ésta constituiría un hecho ilícito es una cuestión sobre la que la mayoría de los Estados aún no se ha pronunciado en términos suficientemente precisos. La Unión se ha esforzado en los últimos años en desarrollar medidas preventivas (continúa, de hecho, haciéndolo), pero también sería aconsejable determinar criterios que ayuden a decidir cuándo una *ciberinjerencia* traspasa el límite de lo legalmente admisible, a fin de elegir la reacción correcta. Por eso la resolución del

[89] HÜSCH, P., "Rerouting Parts of Ukrainian Internet Traffic – A Violation of the Principle of Non-Intervention?", *https://opiniojuris.org/2022/05/10/rerouting-parts-of-ukrainian-internet-traffic-a-violation-of-the-principle-of-non-intervention/*, 10 de mayo de 2022.

[90] Sobre estas cuestiones, MOULIN, T., *óp. cit*., nota 68, p. 432 y TSAGOURIAS, N., "Electoral cyber interference, self determination and the principle of non intervention in cyerspace", 17 agosto 2019, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3438567#:~:text=Nicholas%20Tsagourias,-University%20of%20Sheffield&text=Its%20main%20argument%20is%20that,a%20state's%20authority%20and%20will*


DOI: 10.17103/reei.45.03

Parlamento pedía expresamente, respecto de estos casos (párr. 137), definir con claridad "qué constituye un hecho internacionalmente ilícito" y establecer "unos umbrales mínimos para la puesta en marcha de contramedidas como consecuencia de esa nueva definición (…)".

No parece factible, al menos de momento, materializar esa petición, pues son algunas aún las divergencias entre los Estados miembros. Las Conclusiones del Consejo de 18 de julio de 2022 pedían al Alto Representante y a la Comisión que presentaran opciones "sobre medidas bien definidas que podrían tomarse contra actores FIMI"[91]. La "Política de la UE sobre Ciberdefensa", aprobada en noviembre[92] por la Comisión no fue mucho más generosa en detalles. Peor aún, se alude en ella a ataques que pueden "socavar y perjudicar el funcionamiento de las democracias, incluso atacando las infraestructuras electorales", con lo que se acoge la visión más limitada de injerencia (*ciberinjerencia* material), aunque es cierto que esta Política es sólo un primer paso, dado que su texto finaliza pidiendo al Alto Representante, a la Comisión y a los Estados miembros "medidas prácticas de implementación[93]. Los Informes anuales previstos concretarán y mejorarán, esperamos, esos avances.

El Consejo sí pedía, en sus Conclusiones de 21 de junio de 2022 un mecanismo para adoptar decisiones rápidas "*on a case-by-case basis*", que buscara definir y aprobar propuestas coordinadas. La Unión parece, así, querer unirse a una tendencia ya seguida, por ser la más realista, por varios Estados que, ante la dificultad de soluciones generales y definiciones que logren abarcar la variedad de conductas existentes en el ciberespacio, prefieren una evaluación caso a caso (Canadá[94], Estonia[95], Alemania[96], Noruega[97], Rumanía[98], Suiza[99], Suecia[100] y Países Bajos[101]). Y quizás sea, en efecto, lo razonable, con lo que acaso la Unión debería, como sugería el Parlamento, enfocar sus esfuerzos en

[91] Párr. 6 *in fine*. La Agencia Europea para la Ciberseguridad elaboraba un informe en diciembre de 2022 ("Foreign Information Manipulation Interference and Cybersecurity Threat Landscape", *https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape*) intentando definir de una manera más precisa esas amenazas y proponiendo respuestas de conjunto.
[92] *Óp. cit*., nota 23, p. 2.
[93] *Íd*, p. 21.
[94] *Óp. cit*., nota 41, párr. 21.
[95] Pone como ejemplo expreso de intervención "national democratic processes such as elections, or military, security or critical infrastructure systems (Official compendium*…, óp. cit*., nota 42, p. 25).
[96] Official compendium*…, óp. cit*., nota 42, p. 35 ("For example, it is conceivable that a State, by spreading disinformation via the internet, may deliberately incite violent political upheaval, riots and/or civil strife in a foreign country, thereby significantly impeding the orderly conduct of an election and the casting of ballots (…). A detailed assessment of the individual case would be necessary")*.*
[97] *Íd*, p. 67.
[98] *Íd*, p. 77.
[99] *Íd*, p. 88.
[100] Position Paper on the Application of cyberspace, July 2022, p. 2, disponible en *https://www.regeringen.se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf*
[101] "The precise threshold of what constitute a cyber operation in violation of sovereignty is not settled in international law, and will depend on a case-by-case assessment*",* Official compendium*…, óp. cit*., nota 42, p. 68.


DOI: 10.17103/reei.45.03

diseñar algún mecanismo que ayudara a los Estados a determinar cuándo un supuesto concreto debe considerarse *ciberinjerencia*. Es más, una resolución anterior ya había propuesto fijar la línea entre una mera intervención y una acción mayor que pudiera constituir un ataque armado[102] y cuyas consecuencias irían, por tanto, y así se menciona expresamente, más lejos (legítima defensa y activación de las cláusulas de defensa mutua del artículo 42.7 del TUE y de solidaridad del artículo 222 del TFUE). Fuera como fuese, el Consejo insistía, en su sesión de julio de 2022, que debería ser sólo un mecanismo de ayuda y/u orientación, puesto que la decisión última descansaría en los Estados, que son quienes ostentan la responsabilidad primaria de oponerse a esos ataques[103].

A la espera de una definición, postura o documento que aclare más y mejor el parecer de la Unión (si es que llegara a materializarse), en otras normas podríamos encontrar ideas u orientaciones de lo que, según la UE, podría considerarse como coerción. Así, la propuesta de Reglamento relativo a la protección de la Unión y de sus Estados miembros frente a la coerción económica por parte de terceros países[104] sí establece (art. 2.1) que se aplicará (esto es, que se considerará que existe coerción) cuando un tercer país "interfiera en las decisiones soberanas legítimas de la Unión o de un Estado miembro tratando de impedir o de conseguir la paralización, modificación o adopción de un acto concreto por la Unión o por un Estado miembro". En este caso, se trataría sólo de una interferencia relativa a medidas que afecten al comercio o la inversión, pero algo similar podría aplicarse analógicamente al tipo de situaciones que son objeto de este artículo (injerencias electorales y/o aquellas que tengan lugar en el ciberespacio). En el Reglamento se ofrecen, además, determinados parámetros para determinar si, en efecto, esa coerción está teniendo lugar (art. 2.2) y especialmente interesante resulta el papel de la Comisión, que tiene la última palabra, pues es la encargada de determinar si la misma se ha producido (art. 3)[105] y de adoptar la decisión correspondiente (art. 4) con las medidas que, en su caso, correspondan.

## IV. ¿CÓMO RESPONDER?

### 1. Lo primero, atribuir la acción

Una vez constatado que una *ciberinjerencia* en un proceso electoral constituye un ilícito (por violar el principio de no intervención o el de soberanía), el reto mayor sería, sin duda, la atribución de esa acción a un Estado concreto (artículo 2 del Proyecto de la Comisión de Derecho Internacional, CDI, sobre responsabilidad internacional del Estado por hechos internacionalmente ilícitos de 2001[106]), que resulta mucho más compleja que en un

[102] Res P-9TA (2021)0412, de 7 de octubre de 2021, párr. 32.
[103] Véanse las Conclusiones del Consejo de junio de 2022 (*óp. cit.*, nota 31, párr. 8) y las Conclusiones del Consejo de 18 de julio de 2022 (*óp. cit*, nota 31, párr. 3).
[104] Doc. COM(2021) 775 final, 2021/0406(COD), 8 de diciembre de 2021. El Consejo hacía pública su posición respecto de la propuesta en noviembre de 2022 (doc. 14837/22, 16 de noviembre de 2022).
[105] El Consejo introducía su posición en noviembre de 2022 (*óp. cit*., nota anterior), con buen criterio, creo, que también los Estados pueden solicitar a la Comisión que investigue un posible supuesto de coerción.
[106] Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones (23 de abril a 1.º de junio y 2 de julio a 10 de agosto de 2001, A/56/10, *Anuario de la Comisión de Derecho Internacional*, 2001, vol. II, 2ª Parte, pp. 20-153.


DOI: 10.17103/reei.45.03

entorno analógico. La aplicabilidad de esas normas de responsabilidad al ciberespacio fue aceptada en 2015 por el Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones y también por el Manual de Tallín[107].

En el caso de las *ciberinjerencias* electorales (como, en general, las que se desarrollan en el ciberespacio), los problemas que genera cualquier atribución se complican aún más, por la dificultad de localizar *en las redes* al autor (desde qué ordenador situado en dónde se llevó a cabo la acción y qué nexo existía con un concreto Estado). Pese a todo, la atribución es ineludible para evitar el caos y evitar, como se ha afirmado, que el ciberespacio se convierta en un "salvaje oeste internacional" [108], con continuas perspectivas de escalada e incertidumbre.

Dejando a un lado las atribuciones de carácter técnico y político que los Estados pueden hacer si así lo consideran conveniente ante un acción en el ciberespacio que les perjudica[109], sabemos que, en el plano jurídico, se atribuyen al Estado los hechos llevados a cabo por sus órganos[110] y también los actos de "personas o entidades privadas habilitadas por el propio Estado para ejercer funciones propias del poder público" (art. 5). No obstante, el ciberespacio obliga reinterpretar ciertas premisas, y el Grupo de Tallín lo expuso claramente[111], refiriéndose expresamente a algunas: por ejemplo, ¿y si el *ciberincidente* proviene de una compañía de titularidad estatal que, digamos, es la que se encarga de orquestar manipulaciones de campañas electorales o es la responsable, pongamos por caso, de hackear las máquinas de recuento de votos?, ¿hay que asumir directamente que es atribuible al Estado? Según los expertos del Grupo, habría, entre otras cosas, que comprobar expresamente que, al actuar, esa compañía no estuviera operando dentro de lo que son sus esferas privadas, ajenas a las gubernamentales[112]. La misma reflexión podría hacerse si la *ciberinjerencia* tuviera su origen en instalaciones estatales (bases militares, buques de guerra…)[113]: en el mundo analógico, la atribución sería clara y directa, pero no en el digital.

Sabemos también que al Estado se atribuyen los actos de los "órganos de otro Estado pero que actúan, porque han sido puestos oficialmente a su disposición, siguiendo instrucciones de otro" (art. 6)[114], pero tampoco esta cuestión se libra de cierta

[107] Doc. A/70/74, 22 de julio de 2015 (párr. 28, f) y *Tallinn Manual 2.0, óp. cit.,* nota 34, normas 14 y 17, respectivamente.
[108] TRAN, D., "The law of attribution: rules for attributing the source of a cyber-attack, *Yale Journal of Law and Technology*, vol. 29, 2018, pp. 376-441 (p. 384).
[109] Véase "International Law and cyberspace", Report of the Study Group, *óp. cit*., nota 34, p. 15 y pp. 18 y ss.
[110] Según el artículo 4 del Proyecto de la CDI, *óp. cit*., nota 106.
[111] *Tallinn Manual 2.0 …, óp. cit.*, nota 34, norma 15, pp. 87 y ss.
[112] "(…) Although owned by a State, such entities may have purely private functions, as distinguished from those that perform, at least in part, governmental ones" (*Tallinn Manual 2.0 …, óp. cit.,* nota 34, párr. 5, p. 88).
[113] "… another State or a non-State actor may have acquired control over government cyber infrastructure and is using it to conduct cyber operations." (*Tallinn Manual 2.0 …, óp. cit.,* nota 34, párr. 13, p. 91).
[114] Sobre las dificultades, ya no legales sino técnicas de la atribución (explicadas, además, con claridad), véase TSAGOURIAS, N. y FARRELL, M., "Cyber attribution: technical and legal approaches and challenges", *EJIL*, vol 31, 3, 2020, pp. 941-967 (pp. 947-948).


DOI: 10.17103/reei.45.03

complejidad: ¿acaso no podría alegar el Estado al que se acusara de un hecho ilícito que las acciones (en nuestro caso, *ciberacciones*) de algunos individuos relacionadas con ese Estado se hicieron en la esfera privada?[115]. Quizás el supuesto más problemático es aquel que se contempla en el artículo 8 del Proyecto de la CDI de 2001, según el cual el Estado puede responder asimismo de los actos llevados a cabo por individuos[116]. La posibilidad de que las *ciberoperaciones* de actores no estatales fueran imputables al Estado fue expresamente admitida por el Grupo de Tallín, que prefirió (como también ha hecho la CIJ y la propia CDI) la teoría de *control efectivo*[117] a la del control general. Aunque aquella parece seguir siendo la favorita[118], ya hay quien afirma que apartarse de ella podría ayudar con las dificultades que genera la atribución en el caso de acciones de actores no estatales que tienen lugar en el ciberespacio[119].

Respecto de la atribución, la CIJ ha sido tradicionalmente rigurosa al determinar hasta qué punto podía considerarse que un hecho era imputable al Estado ("*convincing evidence*", "*clear and convincing evidence*"). Pero el Grupo de Tallín fue más abstracto y flexible al afirmar que, cuando surjan dudas respecto de la atribución, los Estados "deben actuar como los Estados razonables actuarían en iguales o similares circunstancias cuando consideraran respuestas a ellos". Esa racionalidad depende del contexto y de, entre otras, la "fiabilidad, cuantía, franqueza, naturaleza (por ejemplo, datos técnicos, inteligencia humana) y la especificidad de la información relevante disponible cuando se considera a la luz de las circunstancias concurrentes y de la importancia del derecho en cuestión"[120]. En un entorno tan peculiar como el ciberespacio y particularmente para los casos de *ciberinjerencias* (no para aquellos que superen ese umbral y pasen a considerarse *ciberataques*) parece, en efecto, que sería conveniente "un parámetro más bajo del de prueba clara y convincente" [121], sobre todo porque resultará probable que el Estado

[115] El caso del GRU (Departamento Central de Inteligencia) ruso y su injerencia en las elecciones de Estados Unidos de 2016 podría ajustarse a esta hipótesis (TSAGOURIAS, N. y FARRELL, M., *óp. cit*., nota anterior, p. 954).

[116]Cuando se trate de acciones de particulares que actúan por cuenta de un Estado o bajo su dirección y control (artículo 8), o cuando se ven impelidos, en ausencia de las autoridades competentes, a hacerse cargo, de atribuciones propias del poder público (artículo 9) y cuando sean actos, en determinadas condiciones, de un movimiento insurreccional (artículo 10). Al respecto, GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, Cizur Menor, 2020, pp. 82-86, párrs. 38-39 y, del mismo autor, *El hecho ilícito internacional*, Dykinson, Madrid, 2005, pp. 79-105.

[117] *Tallinn Manual 2.0 …, óp. cit.,* nota 34, pp. 96-97, norma 17. La teoría del control general, recordemos, fue acuñada por el Tribunal Penal para la ex Yugoslavia (Appeal Judgment, Prosecutor v. Tadic, case ICTY-94-I-A, Appeal Chamber, sentencia de 15 de julio de 1999, párr. 131). Sobre estas cuestiones, MACAK, K., "Decoding article 8 of the International Law Commission's Articles on State Responsability: attribution of cyber operations by non-State actors", *Journal of Conflict and Security Law*, vol. 21, 3, 2016, pp. 405-428 y GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza…, óp. cit.*, nota 116, pp. 86 y 87, párr. 41.

[118] GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza…, óp. cit.*, nota 116, pp. 85-86, párrs. 38-39.

[119] TSAGOURIAS, N. y FARRELL, M., *óp. cit*. nota 114, p. 962.

[120] *Tallinn Manual 2.0 …, óp. cit.,* nota 34, párr. 10, pp. 80 y 81.

[121] Al respecto, MIKANAGI, T. y MAČÁK, K., "Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case", *Cambridge International Law Journal*, vol. 9, 1, p. 15 (disponible en https://ore.exeter.ac.uk/repository/handle/10871/40905). El artículo se centra en un asunto ante tribunales estadounidenses contra el Sr. Park Jin Hyok, un hacker coreano acusado de llevar a cabo varios


DOI: 10.17103/reei.45.03

implicado no quiera cooperar o que la obtención de pruebas claras de atribución directa a ese Estado no resulte sencilla.

Aunque tanto el texto de la CDI como el Manual de Tallín nos ofrecen directrices para determinar cómo podría atribuirse una *ciberoperación*, las carencias aún existentes hacen compleja la rendición de cuentas para quien comete estas acciones, lo que confiere un atractivo añadido a quienes las llevan a cabo, ya sea Estados o individuos. En el ámbito de la Unión Europea, la resolución del Parlamento se hacía eco de ello, al constatar la preocupación "por la ausencia de normas y de medidas apropiadas y suficientes para atribuir los actos de injerencia extranjera y responder a ellos"[122].

Los intentos de la UE por ofrecer unas normas generales de atribución (o, al menos, unos parámetros mínimos), aplicables en todo su territorio, se encontrarían con un problema añadido: los Estados europeos parecen preferir que la decisión final provenga de manera *individual* del Estado afectado, que caso por caso determinará en última instancia si tal injerencia ha existido o no y a qué Estado, en su caso, se atribuye[123]. Y no se percibe que, de momento, y por mucho que la amenaza sea creciente, estén dispuestos a ceder también a la Unión ese reducto de soberanía, en el que aún consideran que bastaría con reforzar la cooperación. La Brújula Estratégica (2022), comulga con esa línea respecto de las amenazas híbridas:

> "Los Estados miembros podrán proponer una atribución coordinada de actividades híbridas, reconociendo que la atribución es una prerrogativa nacional soberana"[124]

Pocos meses después, en las Conclusiones sobre un marco para para una respuesta coordinada de la Unión ante campañas híbridas de junio de 2022, el Consejo insistía:

> "la atribución a un Estado o a un agente no estatal sigue siendo una decisión política soberana basada en información de todas las fuentes y adoptada caso por caso"[125].

Y una ojeada a algunos de los documentos aprobados por los Estados regulando cuestiones del ciberespacio confirma ese sentir. Francia defiende que es una decisión política nacional, aunque "puede ejercerse en coordinación con otros Estados u organizaciones internacionales"[126] (pensando probablemente tanto en la UE como en la

---

ciberataques (entre ellos, el conocido Wannacry) siguiendo órdenes del Gobierno de Corea del Norte y sirve, precisamente, para poner de relieve la dificultad de probar que el Sr. Park recibía órdenes de ese Estado.

[122] Párr. 8 de la resolución del Parlamento Europeo (*óp. cit*., nota 9).

[123] Y es que, en efecto, la atribución es una decisión última que los Estados toman a la vista de las pruebas que tienen para así hacerlo: "Absolute certainty is not -and cannot be-required, pero sí que los Estados "act reasonably…" (EGAN, B. J., "International Law and stability in cyberspace", *Berkeley Journal of International Law*, vol. 35, 1, 2017, pp. 169-180 (p. 177).

[124] *Óp. cit.*, nota 27, p. 22.

[125] *Council Conlusions on a Framework…*, *óp. cit*., nota 31, párr. 17 (también párr. 14).

[126] International law applied to operations in cyberspace. Paper shared by France with the Open-ended working group established by resolution 75/240, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf. De hecho, ya hay varios casos de atribuciones colectivas: la primera fue la realizada conjuntamente por Reino Unido y Países Bajos tras el ataque a la Organización para la Prohibición de las Armas químicas (véase DELERUE, F., *Cyberoperations and International Law*, Cambridge University Press, Cambridge, 2020, pp. 178-181).


DOI: 10.17103/reei.45.03

OTAN), algo en lo que coincide con Finlandia[127], Alemania[128], Italia[129] y Estonia[130]. Este sentir es, de hecho, compartido por Estados fuera de la Unión: Australia[131], Israel[132], Suiza[133] y Reino Unido[134]. Es más, algunos llegan a distinguir expresamente entre atribución desde el punto de vista jurídico, atribución política e identificación técnica de la autoría[135].

Sea como fuere, el Parlamento Europeo estaba en lo cierto: resulta difícil, técnica, política y jurídicamente, atribuir de manera clara una *ciberinjerencia* a un ente estatal en particular y son los Estados los que deciden si correr el riesgo de poner o no el cascabel al gato y llevar esa atribución formal a sus últimas consecuencias. Pero, como también se afirmó, precisamente por esas razones es necesario establecer una serie de criterios mínimos, y no estaría mal que la Unión fuera pionera o, incluso sentara precedente o ejemplo (*Brussel's effect*) en esa tarea: la UE, dice el Parlamento, "debe tomar la iniciativa en el establecimiento de normas internacionales claras para la imputación de injerencias extranjeras"[136]. Eso sí, si la coordinación con otras organizaciones internacionales (OTAN, por ejemplo) es en todo caso altamente recomendable[137], aún lo es más en un mundo tan conectado y sin fronteras visibles como el ciberespacio

Una respuesta ante una *ciberinjerencia* pasaría, claro está por arbitrar algún método de arreglo específico de controversias. Aun a sabiendas de que un análisis de esta opción excedería de las páginas de este artículo, no me resisto a plantear, al menos mínimamente, una posibilidad: que el acto formal de la atribución recayera en alguna institución u organismo de la Unión (preferentemente, el que ya se propuso para determinar si había existido o no una *ciberinjerencia* constitutiva de hecho ilícito internacional), mediante un procedimiento preestablecido dirigido preferentemente por la Comisión y que, de ser posible, finalizara con un dictamen obligatorio. El valor de ese organismo residiría en que contaría con los expertos necesarios para ello (de lo que se beneficiarían todos los Estados

---

127 Véase https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

128 Cuya opinión sobre la atribución de una *ciberoperación* coincide de manera prácticamente plena con la del Grupo de Tallín (*On the application of*…, *óp. cit.*, nota 48).

129 Italian Position Paper*…, óp. cit.*, nota 44.

130 Official compendium*… óp. cit.*, nota 42, p. 28.

131 "Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber activities to another State" (*óp. cit.*, nota 79).

132 Consúltese en https://digital-commons.usnwc.edu/ils/vol97/iss1/21/

133 Federal Department of Foreign Affairs, Switzerland's position paper on the application of International Law in cyberspace, May 2021, pp. 5-6.

134 Que se reserva, además, la decisión de hacer pública o no esa atribución, United Kingdom Foreign, Commonwealth, Development Office, Application on International Law to States's conduct in cyberspace, UK Statement, 3 June 2021.

135 Canadá: "Attribution in its legal sense is of course distinct from the technical identification (or technical attribution) of the actor responsible for malicious cyber activity, whether State or non-State, as well as from the public denunciation of the responsible actor (political attribution)" (International Law aplicable to cyberspace, *óp. cit.*, nota 41). En la misma línea, Países Bajos (Government of the Kingdom of the Netherlands, Appendix: International Law in cyberspace, 26 September 2019, pp. 6-7), Suecia (*óp. cit.*, nota 100, p. 5) y Estados Unidos (Official compendium..., *óp. cit.*, nota 42, pp. 141-142).

136 Párr. J de la resolución (*óp. cit.*, nota 9).

137 También lo señala la resolución del Parlamento, *óp. cit.*, nota 9, párr. 142.


DOI: 10.17103/reei.45.03

miembros, con independencia de su desarrollo tecnológico) y que las técnicas y métodos serían iguales para todos, con lo que al menos podrían generalizarse ciertas pautas de atribución. Algún autor ya proponía algo en este sentido a nivel internacional, reconociendo enseguida, desde luego, la dificultad de que todos los Estados cooperaran en una cuestión tan vinculada a la soberanía[138]. ¿No sería más factible implantarlo en la Unión y exportarlo después, si los resultados fueran satisfactorios, a otras organizaciones o grupos de Estados? Puede que, incluso, de ser la experiencia positiva, muchos recelos se mitigaran.

Las dificultades apuntadas han sido, probablemente, las culpables de que, frente a otros opciones, gane terreno, en la UE pero también entre algunos Estados, como respuesta formal ante *ciberoperaciones*, la adopción de medidas restrictivas dirigidas expresamente contra *individuos* y no contra Estados directamente (contramedidas *stricto sensu*), en tanto en cuanto las consecuencias políticas y diplomáticas de *acusar* a alguien (individuo, entidad) son menores que las de culpar directamente a un Estado (*vid infra* apartado 2, B).

Una opción alternativa, que ayudaría a superar esos problemas de atribución, sería generalizar la aplicación de la norma de la *diligencia debida*, que obliga a los Estados a responsabilizarse de lo que ocurra (en este caso, *ciberinjerencias*) dentro de su territorio o en las zonas bajo su jurisdicción[139]. El Informe de 2015 del GGE, adoptado por consenso, aun admitiéndola[140], la califica expresamente como norma no vinculante, pero el Grupo de Tallín aceptó su carácter consuetudinario[141]. También los Estados se

[138] TSAGOURIAS, N. y FARRELL, M. *óp. cit*, nota 114, pp. 959-960. Una Agencia de Atribución Internacional, proponían, aunque su creación, afirman, sería "quite premature" (p. 961) y, además, "will just add another layer".

[139] El concepto tiene su origen en el arbitraje de la isla de Las Palmas, *óp. cit*., nota 33, p. 839. Posteriormente, la CIJ lo confirmaría en el asunto del Canal de Corfú, 9 de abril de 1949 (*ICJ Reports 1949*, p. 22 y declararía su naturaleza consuetudinaria en el asunto sobre la legalidad de la amenaza o el empleo de armas nucleares (*ICJ Reports 1996*, p. 226, párr. 2). Sobre el concepto, en general, LOZANO CONTRERAS, J. F., *La noción de debida diligencia en Derecho Internacional Público*, Atelier, Barcelona, 2007 (pp. 41 y ss.).

[140] Doc. A/70/174, 22 de julio de 2015, párr. 13 c.

[141] "…los Estados no deberían permitir a sabiendas que su territorio se use para hechos ilícitos internacionales usando TIC's", *Tallinn Manual 2.0 …, óp. cit.,* nota 34, pp. 43 y 30. Un completo estudio de la cuestión, en COCO, A. y DE SOUZA DIAS, T., "Cyber due diligence: a patchwork of protective obligations in International Law*", EJIL*, vol. 32, 3, 2021, pp. 771-805. Los autores proponen hablar más bien de "obligaciones protectoras" (obligación de proteger otros Estados e individuos de *ciberdaños*), basadas a su vez en varias normas primarias del Derecho Internacional (véase p. 774), como la obligación de prevenir ciberataques contrarios a los derechos de otros Estados, la obligación de prevenir daños transfronterizos o la obligación de respetar los derechos humanos o el Derecho Internacional Humanitario. Por su parte, la *Declaración de Oxford sobre la protección del Derecho Internacional contra la injerencia electoral extranjera por medios digitales* también aboga la diligencia debida (párr. 5, *https://www.ejiltalk.org/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through-digital-means*/). Véase asimismo CHIRCOP, L., "A due diligence standard of attribution in cyberspace", *International and Comparative Law Quarterly*, vol. 67, July 2018, pp. 643-668 (que propone que opere como norma secundaria, pp. 645 y 653-654) y COCCHINI, A., "Ciberdiligencia debida: ¿una actuación necesaria para el Derecho Internacional del ciberespacio", *Análisis del Real Instituto Elcano 27/2001*, 2 de marzo de 2021, pp. 1-5 (pp. 3-5).


DOI: 10.17103/reei.45.03

muestran divididos respecto a la naturaleza jurídica de la diligencia debida. Mientras que la mayoría de los europeos (y alguno más, como Japón)[142] la consideran una norma de carácter obligatorio perfectamente aplicable al ciberespacio, otros (Estados Unidos[143], Reino Unido[144], Australia, Canadá, Israel o Nueva Zelanda)[145] siguen sin aceptarla[146].

La cuestión es ciertamente compleja en un entorno como el ciberespacio. Por ejemplo, y por referirnos a algún supuesto de los incluidos en el objeto de este trabajo: en el caso de una campaña de desinformación a través de una red social, que ha logrado dar la vuelta a unos resultados electorales, ¿quién sería el titular de esa diligencia debida? ¿el Estado desde el que opera la compañía titular de esa red? ¿el Estado desde el que distintos usuarios expresaron sus opiniones?, ¿la compañía, por no controlar el contenido de esas opiniones? Idénticos problemas surgirían en otros supuestos que incluyeran una injerencia más obvia (manipulación directa del sistema de recuento de votos, pongamos por caso), y en los que determinar quién tenía la obligación de evitar la acción sigue siendo complejo.

Generalizar la norma de diligencia debida en el ciberespacio permitiría, sí, evitar las "etiquetas" formales de quién hizo qué y si la acción era atribuible o no al Estado. Para eludir la responsabilidad bastaría con probar que se actuó *diligentemente*, pero también es cierto que ese matiz encierra otro gran problema: ¿cómo interpretar que se obró así?, ¿qué *esfuerzos* del Estado serían necesarios?, ¿podríamos exigirlos por igual a aquellos menos avanzados tecnológicamente?[147] Sea como fuere, aún quedan muchos a quienes convencer de las bondades de esta norma.

## 2. Lo segundo, las consecuencias

### A) DE LAS CONTRAMEDIDAS…

Una *ciberinjerencia* que violara el principio de soberanía o el de no intervención, una vez atribuida a un Estado, constituiría un hecho ilícito internacional frente al cual el Estado afectado podría reaccionar, dentro de los márgenes que le impone el Derecho

---

[142] Official compendium…, *óp. cit.*, nota 42, p. 48.
[143] "The United States has not identified the State practice and opinio juris that would support a claim that due diligence currently constitutes a general obligation under international law*",* Official compendium …, *óp. cit.*, nota 42, 13 de julio de 2021, p. 141.
[144] "…there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace", Official compendium…, *óp. cit.*, nota 42, 13 de julio de 2021, p. 117.
[145] "Whether this norm also reflects a binding legal obligation is not settled…", *The application of International Law to State activity in cyberspace*, *óp. cit.*, nota 80, p. 3
[146] SCHMITT, por ejemplo, considera que la norma existe, pero que otra cosa es si resulta aplicable (él cree que sí) al ciberespacio, *óp. cit.*, nota 50. Del mismo autor, "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum*, vol. 125, 2015, *http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace*.
[147] No extraña por tanto que muchos autores se muestren escépticos ante la eficacia de este elemento en el ciberespacio. Al respecto, véase CORTÉS MARTÍN, J. M., "Ciberataques y responsabilidad…", *óp. cit.* nota 76, pp. 60-61.


DOI: 10.17103/reei.45.03

internacional. En el marco de las respuestas más factibles, y dejando otras a un lado, por razones de tiempo y de espacio[148], encontraríamos las contramedidas[149].

La adopción de contramedidas en el ciberespacio fue admitida por el Grupo de Expertos del Manual de Tallín[150], que las somete, en grandes líneas, a las exigencias generales fijadas para ellas por el Proyecto de artículos sobre responsabilidad internacional de los Estados de la CDI y confirmadas luego por la CIJ[151]: deben ser respuestas frente a hechos ilícitos previos, tener una finalidad no punitiva (reversibles, pues), notificadas previamente, proporcionales, su adopción es sólo posible por el Estado directamente lesionado (salvo, podría alegarse, que se trate de la violación de normas colectivas o que afectan a la comunidad internacional en su conjunto[152]) y han de ir dirigidas contra el Estado que causó el hecho que las desencadenó.

Muchos Estados ya han confirmado estar dispuestos a recurrir a las contramedidas en el ciberespacio[153], pero lo cierto es que los requisitos aplicables condicionan no poco su puesta en marcha, particularmente el que sólo puedan ejercerse contra una entidad estatal y que su autor tenga que ser el Estado directamente lesionado. ¿Y si el Estado afectado, en nuestro caso, por una injerencia electoral llevada a cabo en el ciberespacio, no posee la capacidad tecnológica suficiente para contrarrestarla y responder? Algún Estado ha dado ya los primeros pasos para romper esa rigidez, admitiéndolas también para acudir en ayuda de un Estado tercero que así lo solicite[154] y también el Parlamento de la UE

[148] Podría invocarse también, en caso de que la respuesta a esa *ciberinjerencia* fuera a su vez un ilícito, el estado de necesidad, pero habría que examinar cuidadosamente las condiciones para hacerlo.

[149] Sobre contramedidas en general GUTIÉRREZ ESPADA, C., *La responsabilidad internacional (consecuencias del ilícito)*, Diego Marin Ediciones, Murcia, 2005, pp. 164-218; GUTIÉRREZ ESPADA, C., CERVELL HORTAL, Mª. J., *Derecho Internacional (corazón y funciones)*, Aranzadi, 2022, pp. 348-364; BENNOUNA, M., *Le Droit international entre la lettre et l'esprit, The pocketbooks of The Hague Academy of International Law*, Brill, M. Nijhoff, La Haya, 2017, pp. 135-136 y KOLB, R., "Le Droit International comme corps de 'Droit privé' et de 'Droit public'. Cours general de Droit International Public", *Recueil des Cours/Collected Courses*, vol. 419, 2021, pp. 9-668, pp. 319-355.

[150] Véase la norma 20 del Manual de Tallín, *óp. cit*,. nota 34, pp. 111-116.

[151] Asunto Gabcikovo Nagymaros, sentencia de 2 de septiembre de 1997, *ICJ Reports 1997*, pp. 55-57. Sobre contramedidas en el ciberespacio GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza …*, *óp. cit.*, nota 116, pp. 131-137; del mismo autor, "La creciente necesidad de legislación contra las amenazas cibernéticas, fuentes de graves daños transnacionales", *Cuadernos de Derecho Transnacional*, vol. 14, 2, octubre 2022, pp. 10-46, pp. 30-37. También SCHMITT, M. N., "Below the threshold cyberoperations: the countermeasures response option and International Law", *Virginia Journal of International Law*, vol 54, 3, 2014, pp. 697-732.

[152] *Vid*. artículo 48 el Proyecto de la CDI sobre responsabilidad internacional de los Estados (*óp. cit*., nota 106).

[153] Por ejemplo, Australia, Estonia, Francia, Alemania, Holanda, Reino Unido, Nueva Zelanda, Japón y Estados Unidos.

[154] *Ad. ex*., Estonia (*Opening address (President of Estonia) at the 11th International Conference on Cyber Conflict (CyCon) in Tallinn*, 29 de mayo de 2019, *https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon*) y Nueva Zelanda: "New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures …" (*The application to International Law to State activity in Cyberspace…, óp. cit.,* nota 80). Sobre la rigidez de las contramedidas en el ciberespacio, SCHMITT, M. N., "Below the threshold cyberoperations…", *óp. cit*., nota 151, p. 73.


DOI: 10.17103/reei.45.03

parece considerarlo conveniente[155]. ¿Se abre paso, al menos en ciertos supuestos del ciberespacio, a la adopción de contramedidas por Estados terceros, distintos del lesionado? De momento, el número de Estados que lo acepta abiertamente es demasiado limitado como para hablar de un cambio de tendencia, pero lo cierto es que admitir esas contramedidas a favor de Estados terceros que no pudieran por sí mismos, reaccionar ante *ciberoperaciones*, no sería tan descabellado. Siempre, claro está, dentro de los límites de la proporcionalidad.

No es el único de los requisitos que comienza a ser cuestionado: también la notificación previa, que exige el artículo 52 del Proyecto de artículos de la CDI, es puesta en duda ya por algunos Estados (Finlandia, Francia, Holanda, Italia…), que son de la opinión de que en un entorno como el ciberespacio sólo las respuestas rápidas pueden evitar males mayores. Y no dejan de estar en lo cierto: si un Estado constata, digamos, que en el día de unas elecciones las máquinas de voto están siendo *hackeadas*… y está seguro de esa acción proviene de un Estado concreto ¿de veras ha de cumplir con el requisito de notificación previa para que su respuesta se ajuste a los parámetros de legalidad establecidos?

En todo caso, adoptar contramedidas parece ser la salida natural en muchos casos y las opciones son variadas: aunque en principio podría ser más lógico que esa respuesta fuera también en el ámbito ciberespacial (por ejemplo, una *ciberoperación* de respuesta para desactivar un programa que esté manipulado resultados electorales o dirigida contra *ciberinfraestructuras* distintas de las directamente implicadas en la operación hostil)[156], nada impediría que fuera también una respuesta de carácter *analógico*.

### B) … A LAS MEDIDAS RESTRICTIVAS QUE PARECE PREFERIR LA UNIÓN EUROPEA

Las limitaciones de las contramedidas como reacción a una *ciberinjerencia* han quedado patentes también dentro del marco de la Unión Europea. No en vano, la resolución del Parlamento aboga por la imposición de medidas restrictivas, dirigidas no contra un Estado, sino contra particulares u organismos no estatales. De hecho, la UE ya tiene cierta experiencia en el ámbito del ciberespacio: la Decisión (PESC) del Consejo, de 17 de mayo de 2019, y el Reglamento (UE) 2019/796 del Consejo[157], de la misma fecha, se ocupan de las medidas restrictivas (limitadas, pues sólo se contempla la prohibición de entrada de personas a la Unión y la inmovilización de activos de personas y entidades) contra los ciberataques que amenazan a la Unión o a sus Estados miembros. Las primeras se dieron el 30 de julio de 2022 en respuesta a varios ataques, entre ellos el que sufriera la Organización para la Prohibición de las Armas Químicas. Pero esta

[155] "…la Unión debe esforzarse por encontrar una solución (…) de modo que (…) se autorizasen contramedidas colectivas de los Estados miembros de la Unión con carácter voluntario" (Resolución P9_TA(2021)0412, de 7 de octubre de 2021).
[156] SCHMITT, M. N., "Foreign cyber interference in elections: an international law Primer, Part III", *EJIL Talk*, 19 octubre de 2020.
[157] DOUE L 129 I, de 17 de mayo de 2019, p. 13 y DOUE L 129 I, de 17 de mayo de 2019, p. 1, respectivamente.


DOI: 10.17103/reei.45.03

normativa europea no sería, pese a que contempla también la intromisión en datos o sistemas de información, aplicable en todo caso a las *ciberinjerencias*, pues está destinada más bien a *ciberoperaciones* "con efecto significativo" (artículo 1 de ambas normas), ajustadas los parámetros que recoge el artículo 2 y que, en su mayor parte, excederían de lo que sería una mera *ciberinjerencia*[158].

La resolución del Parlamento Europeo de marzo de 2022 aboga por seguir esa línea y establecer, en casos de injerencia en procesos electorales y desinformación (incluido el ciberespacio), un régimen (¿quizás bastaría con una reforma de la normativa de 2019 ya mencionada para cubrir supuestos por debajo del umbral que ésta fija?) que incluya sanciones diplomáticas, prohibiciones de viaje, inmovilizaciones de activos y retirada de permisos de residencia de la Unión de extranjeros y sus familias[159]. Deben dirigirse con la mayor precisión posible contra los responsables de la toma de decisiones y los organismos responsables y adoptarse, en principio, en coordinación con otras organizaciones internacionales, en particular la OTAN, a la que menciona expresamente en el párr. 142.

La Brújula Estratégica adoptada unos días después es, sin embargo, más abstracta, limitándose a señalar que "desarrollaremos el conjunto de instrumentos de la UE para afrontar y atajar la manipulación de información y la injerencia por parte de agentes extranjeros (…). También impulsaremos el mecanismo operativo conjunto para apoyar los procesos electorales, incluyendo quizá las infraestructuras electorales entre las infraestructuras críticas".

Escueto fue también el Consejo en su sesión de junio de 2022, que no va más allá de aceptar que frente a campañas híbridas pueden activarse medidas restrictivas. No menciona expresamente otras opciones, pero sí invita al Alto Representante y a la Comisión a hacerlo[160].

¿Medidas restrictivas (contra individuos o entidades) o contramedidas (contra un Estado como respuesta a su ilícito previo) para reaccionar ante una *ciberinjerencia* con origen estatal? Lo cierto es que, como dijimos, el Parlamento aboga por lo primero, como también hacen otros Estados fuera de la Unión[161].

---

[158] Un estudio en profundidad de estas normas, en PIERNAS LÓPEZ, J. J, *Ciberdiplomacia y ciberdefensa en la Unión Europea*, Aranzadi, Cizur Menor, 2020, pp. 102-140 y (del mismo autor), "The European Union as an international actor in cybersecurity", *Cuadernos de Derecho Transnacional*, vol. 14, 2, octubre 2022, pp. 712-736 (pp. 722-725). También, ROBLES CARRILLO, M., "Sanciones contra ciberataques: la acción de la Unión Europea", *Documento Opinión 143/2020*, Instituto Español de Estudios Estratégicos, 10 de noviembre de 2020, pp. 1-22. Sobre normativa europea, pero anterior al Reglamento citado, MILLÁN MORO, L., "La respuesta de la Unión Europea a los ciberataques", en MILLÁN MORO, L. (dir.) y Fernández Arribas, G. (ed.), *Ciberataques y ciberseguridad en la escena internacional*, Aranzadi, 2019, pp. 119-147.

[159] Párr. 137 de la resolución, *óp. cit*., nota 9.

[160] *Council Conclusions on a Framework*…, *óp. cit*., nota 31, párrs. 14 y 21, respectivamente.

[161] Estados Unidos, en abril de 2021, anunciaba una conjunto de sanciones por los intentos de influir en las elecciones de 2020 (*Foreign threats to the 2020 US Federal Elections*, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf). Véase también


DOI: 10.17103/reei.45.03

La gran ventaja de estas medidas dirigidas a particulares, además de su fin disuasorio y de que permiten sortear los problemas de atribución estatal, es que, llegado el caso y una vez aclarada la atribución, los Estados (o la propia Unión) aún podrían decidir llegar más lejos y adoptar contramedidas *stricto sensu*[162]. Claro que, por otro lado, las contramedidas sólo pueden ir dirigidas contra Estados, con lo que serían inoperantes en el caso de *ciberinjerencias* llevadas a cabo por grupos *no estatales*[163]. Y aunque acaso no esté de más recordar que el Manual de Tallín 2.0 no rechaza de pleno las contramedidas contra actores no estatales, "especialmente en situaciones en las que ningún Estado es responsable por la *ciberoperación* maliciosa en cuestión"[164], tampoco debe olvidarse que no hay constancia expresa oficial de que los Estados las acepten, en este caso, sin más y en un número suficientemente amplio.

Con todo, el Parlamento es consciente de que "dirigirse a particulares podría no ser suficiente" y que, para proteger los procesos democráticos patrocinados por Estados se podrían utilizar otras herramientas, como las medidas comerciales contra un Estado[165]. Son, pienso, varias las razones que le mueven a admitir que esas medidas restrictivas contra individuos no bastan:

- La eficacia real de estas medidas, adoptadas en cuestiones de ciberespacio (ciberataques) a raíz del Reglamento 2019/796, ha demostrado ser limitada. Hasta la fecha, sólo ocho individuos y cuatro entidades han sido sancionados.[166]
- Castigar a individuos puede ser diplomáticamente menos peligroso, pero el impacto ha sido mínimo: las prohibiciones de viaje o las inmovilizaciones de activos de quienes hasta ahora figuran en la lista de sancionados por la aplicación de la normativa sobre ciberataques no han hecho que Rusia, China o Corea del Norte dejen de recurrir a operaciones en el ciberespacio[167]. Si es un Estado el que está detrás de esas acciones, porque es el aparato estatal el que quiere intervenir en los procesos democráticos de otro Estado, sólo medidas de mayor calado tendrán, en su caso, algún impacto y por eso el Parlamento sugiere la adopción de sanciones comerciales directas contra el Estado en cuestión.
- La exigencia de la unanimidad en las votaciones de esas medidas quizás sea otra causa más que ha provocado que su número haya sido, hasta ahora, escaso en relación con los ciberataques que los Estados Miembros de la Unión Europea han

SCHMITT, M. N., "Foreign cyber interference in elections", *International Law Studies,* vol 97, 2021, pp. 739-764, p. 762.

[162] GUTIÉRREZ ESPADA, C., "La creciente necesidad de legislación contra…", *óp. cit*. nota 151, p. 30.

[163] *Tallinn Manual 2.0 ..., óp. cit.,* nota 34, p. 113, comentario 7. El problema de no poder ejercer contramedidas contra un actor no estatal se acrecienta en el ciberespacio, con lo que algún autor considera que quizás las *cibercontramedidas* puedan tener un "papel preponderante en ese cambio" (CORN, G. y JENSEN, E., "The use of force and cyber countermeasures", *Temple International Law and Comparative Law Journal*, vol. 32, 2, 2018, pp. 127-133, p. 132).

[164] *Tallinn Manual, óp. cit*., nota 34, pp. 113-114, comentario 8 a la norma 20.

[165] Párr. CJ de la resolución, *óp. cit*., nota 9.

[166] Véase Decisión del Consejo 2019/797 (DOUE de 17 de mayo de 2019) y las sucesivas enmiendas para ampliar la lista de sancionados (la última publicada en el DOUE de 17 de mayo de 2022) y prorrogar el tiempo de aplicación (18 de mayo de 2025).

[167] En esa línea, véase PIERNAS LÓPEZ, J. J., "The European Union ...", *óp. cit*. nota 158, p. 733 y la bibliografía citada por el autor.


DOI: 10.17103/reei.45.03

sufrido. El Parlamento Europeo sugiere (párr. 137), de hecho, que en las cuestiones relacionadas con injerencia y desinformación, las decisiones se adopten por mayoría y no por unanimidad. Es más, el 9 de junio de 2022 aprobaba una resolución para dar un paso más en ese sentido[168].

-

Generalizar las contramedidas como reacción a *ciberoperaciones* que supongan un ilícito podría ser más efectivo, pero también obligaría a los Estados a ser tremendamente cuidadosos a la hora de justificarlas, sobre todo al calificar la acción como hecho ilícito porque, como ya apuntamos al hilo de otras reflexiones (*supra* apartado III.2 y IV.1), no siempre es fácil trazar la delgada línea que separa una (ciber)injerencia que viole el Derecho internacional de otra que no lo haga[169]. El mecanismo propuesto en páginas anteriores (*supra* IV.1) que, en el ámbito europeo, se encargaría de decidir esas cuestiones, podría resultar útil a tal efecto.

## V. CONCLUSIONES

Las *ciberinjerencias* en procesos democráticos se han revelado como un problema que crece en magnitud y para el que aún no hay respuestas satisfactorias en el plano jurídico internacional y europeo. El Parlamento Europeo intentaba, en marzo de 2022, dar un paso para aclarar la postura de la Unión en este sentido y definir respuestas concretas, pero lo cierto es que, desde entonces y aún a la espera de que avancen más los trabajos del Comité que actualmente se ocupa de la cuestión, la imprecisión sigue siendo la tónica dominante.

Este artículo ha intentado determinar si una acción que, a través del ciberespacio, pretenda influenciar algún proceso electoral, podría ser etiquetada como hecho ilícito internacional y cuáles serían las consecuencias. Son dos los principios básicos que, en principio, resultarían conculcados: el de no intervención y el de soberanía. En el caso del primero, continuar con una concepción cerrada y tradicional del elemento coercitivo (necesario para poder hablar de violación del principio), no permitirá dar respuestas jurídicas adecuadas. En efecto, mientras que acciones dirigidas directamente a viciar el recuento de votos u operaciones contra sistemas directamente implicados en un proceso electoral (*ciberinjerencias materiales*) resultarían claramente contrarias al mismo, mayores problemas suscitan otro tipo de conductas, como la manipulación de la información que se da al electorado (*ciberinjerencias inmateriales*), en las que la presencia del elemento coercitivo no resultaría tan clara. Flexibilizar ese requisito y dar entrada también a este tipo de acciones, parece necesario para poder hacer frente a las de cierta entidad y escala, que podrían dar un vuelco inesperado e indeseado a procesos electorales. Algunos Estados han empezado ya a aceptarlo de manera expresa. En el caso del segundo (principio de soberanía), es cierto que su gran baza es que no se exige en él la presencia de elemento coercitivo alguno, pero los Estados deben ser conscientes de que admitir su aplicación en

[168] Se trata de una resolución sobre la convocatoria de una convención para la revisión de los Tratados, en la que, entre otras cosas, proponía formalmente el paso a una mayoría cualificada en cuestiones relacionadas con sanciones económicas y financieras, doc. 2022/2705(RSP), párr. 6.
[169] SCHMITT, M., "Foreign cyber interference…", *óp. cit.*, nota 156.


DOI: 10.17103/reei.45.03

el ciberespacio les obligará también en las acciones ofensivas, en las que su margen de actuación se verá irremediablemente limitado.

El guante que arrojaba el Parlamento Europeo en marzo de 2022 se centraba fundamentalmente en la necesidad de que la Unión defina con claridad cuándo una injerencia en procesos electorales sería un hecho ilícito (qué normas se violarían conforme al Derecho Internacional) y cómo atribuir esa acción a un Estado, para así poder definir los métodos de reacción y defensa. Un mecanismo diseñado *ex profeso* para injerencias y desinformación (aplicable también a las que tuvieran lugar en el ciberespacio), controlado de algún modo por la Comisión y en el que se estableciera claramente qué ha ocurrido y quién es el culpable, sería de gran ayuda para guiar a los Estados miembros. La insistencia de los Estados de la Unión en que deben ser ellos quienes tengan la última palabra, podría obligar a hacer sacrificios, como que la decisión final de este mecanismo fuera meramente recomendatoria, pero el implantarlo no debería ser excesivamente problemático: el objetivo final es ofrecer instrumentos a los que aferrarse a la hora de reaccionar frente a *ciberinjerencias* que hagan tambalear la estabilidad democrática y tener así cierto apoyo institucional europeo cuando se decida actuar. Trasladar esa iniciativa fuera de la Unión Europea sería difícil, pero quizás no impracticable si la idea va calando con el ejemplo.

El Parlamento abogaba, además, ya en el plano reactivo, por imponer medidas restrictivas contra individuos en caso de injerencias en procesos electorales. Aun reconociendo que son más factibles por varias razones (no hay que atribuir la acción a un Estado, no se toman como afrentas directas a Gobiernos concretos…), debemos ser conscientes de que las llevadas a cabo hasta ahora en otros ámbitos (ciberataques, por ejemplo) no han sido garantía de éxito. Por eso el Parlamento sugería ir un poco más lejos y considerar sanciones comerciales directamente contra los Estados e, incluso, abandonar la unanimidad a la hora de votarlas. No parece mala opción, por más que de momento se adivine impracticable. En todo caso, la coyuntura internacional actual es la óptima para avanzar, como quizás antes nunca se hubiera imaginado, en este ámbito.

No será fácil, en suma, poder hablar en un futuro cercano de normas claras que resuelvan las manipulaciones que, vía ciberespacio, han sufrido algunos procesos electorales en los últimos tiempos, pero resulta necesario e ineludible empezar a barajar opciones que ayuden a encarar mejor este tipo de problemas. ¿Y por qué no podría la Unión Europea liderar el proceso?


DOI: 10.17103/reei.45.03