

ESTUDIOS

EL DERECHO INTERNACIONAL Y LAS CONTRAMEDIDAS CIBERNÉTICAS

JUAN JORGE PIERNAS LÓPEZ



III ARANZADI

© Juan Jorge Piernas López, 2024
© Editorial Aranzadi, S.A.U.

Editorial Aranzadi, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@aranzadilaley.es
<https://www.aranzadilaley.es>

Primera edición: 2024

Publicación financiada por el Proyecto: «La búsqueda de una regulación internacional para las actividades cibernéticas: ¿una ineludible necesidad? (CYBINREG)», ayudas a proyectos de I+D+i 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), Ref PID 2020 112577 RB-I00.



Depósito Legal: M-26425-2024
ISBN versión impresa: 978-84-1162-868-6
ISBN versión electrónica: 978-84-1162-869-3

Diseño, Preimpresión e Impresión: Editorial Aranzadi, S.A.U.
Printed in Spain

© **Editorial Aranzadi, S.A.U.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Editorial Aranzadi, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

EDITORIAL ARANZADI no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, EDITORIAL ARANZADI se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

EDITORIAL ARANZADI queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

EDITORIAL ARANZADI se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Editorial Aranzadi, S.A.U.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

Índice General

	<i>Página</i>
PRESENTACIÓN.....	13
ABREVIATURAS.....	15
PARTE PRIMERA	
LAS CONTRAMEDIDAS COMO PARTE DE LA AUTOTUTELA EN DERECHO INTERNACIONAL EN EL CIBERESPACIO	17
I. Introducción	17
II. Las contramedidas como parte de la autotutela en el Dere- cho internacional del ciberespacio	19
PARTE SEGUNDA	
PRINCIPALES REQUISITOS DE LAS CONTRAMEDIDAS....	23
I. Requisitos sustantivos.....	26
1. <i>Las contramedidas sólo se deben adoptar en respuesta a un hecho internacionalmente ilícito previo de otro Estado</i>	<i>26</i>
1.1. El principio de no intervención.....	35
1.2. El principio de debida diligencia	47
2. <i>Las contramedidas deben respetar el principio de proporcio- nalidad</i>	<i>61</i>
3. <i>Las contramedidas deben ser reversibles y terminar tan pron- to como el Estado responsable haya cumplido sus obligaciones internacionales</i>	<i>67</i>

	<i><u>Página</u></i>
4. <i>Las contramedidas no pueden afectar a ciertas obligaciones internacionales</i>	71
4.1. <i>Obligaciones internacionales a las que se refiere el artículo 50.1 del Proyecto de artículos</i>	71
4.2. <i>Obligaciones internacionales a las que se refiere el artículo 50.2 del Proyecto de artículos</i>	85
II. Requisitos procesales	89
1. <i>Solicitud de reparación y notificación</i>	89
2. <i>Posibilidad de adoptar contramedidas urgentes sin notificación previa ni oferta de negociación</i>	94
 PARTE TERCERA	
LAS CONTRAMEDIDAS DE TERCEROS Y CONTRA TERCEROS	101
 PARTE CUARTA	
OTRAS MEDIDAS DE AUTOTUTELA APLICABLES FRENTE A CIBERATAQUES	111
I. La retorsión y la legítima defensa frente a ciberataques	111
1. <i>Las medidas de retorsión</i>	111
2. <i>La legítima defensa en respuesta a ciberamenazas</i>	115
 PARTE QUINTA	
LAS CONTRAMEDIDAS EN EL DERECHO DE LA UNIÓN EUROPEA	131
I. Introducción: la postura de la Unión Europea sobre la aplicación del Derecho internacional en el ciberespacio	131
II. La Unión Europea y las contramedidas colectivas	138
1. <i>El Reglamento (UE) 2023/2675: consolidación de la postura de la UE</i>	142
2. <i>La reciente postura del Tribunal General de la UE</i>	149

ÍNDICE GENERAL

Página

PARTE SEXTA

PRINCIPALES CONCLUSIONES	153
BIBLIOGRAFÍA	159

Las contramedidas como parte de la autotutela en Derecho internacional en el ciberespacio

SUMARIO: I. INTRODUCCIÓN. II. LAS CONTRAMEDIDAS COMO PARTE DE LA AUTOTUTELA EN EL DERECHO INTERNACIONAL DEL CIBERESPACIO.

I. INTRODUCCIÓN

El pasado 7 de diciembre de 2023, el Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, realizó una declaración en nombre de la Unión sobre la protección de los procesos democráticos contra las actividades cibernéticas malintencionadas. La declaración condenaba firmemente este tipo de actividades dirigidas contra las instituciones democráticas y los procesos electorales, y mostraba su solidaridad con el Reino Unido, que ese mismo día había acusado al Servicio de Seguridad ruso, el FSB, de una campaña sostenida de ciberhackeo dirigida contra políticos y otros cargos públicos. La Unión Europea y sus Estados miembros, concluía la declaración, se muestran dispuestos a emprender cualquier acción necesaria de ciberdiplomacia, incluida la imposición de sanciones, para prevenir y responder a ciberataques inaceptables¹.

La declaración es ilustrativa de un contexto como el actual, en el que los ciberataques representan una creciente amenaza para la seguridad global, así como para los procesos electorales democráticos en todo el mundo. En

1. La declaración institucional puede consultarse (en inglés) en el siguiente enlace: https://www.consilium.europa.eu/es/press/press-releases/2023/12/07/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-the-protection-of-democratic-processes-against-malicious-cyber-activities/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cyber:+Statement+by+the+High+Representative+on+behalf+of+the+European+Union+on+the+protection+of+democratic+processes+against+malicious+cyber+activities

la reunión de Davos celebrada a inicio de 2023 se presentó un informe del *World Economic Forum* que afirma que más del 93% de los expertos en ciberseguridad y el 86% de los líderes empresariales creen que «es probable que se produzca un acontecimiento cibernético catastrófico de gran alcance en los próximos dos años»². La situación previsiblemente se agravará con la creciente conexión de dispositivos a Internet a través del denominado Internet of Things (IoT), que prevé la conexión de más de 41 mil millones de dispositivos IoT para 2025³. Además, la situación de la Unión Europea es particularmente complicada, habida cuenta de que es un importador neto de productos y servicios de ciberseguridad, y depende en gran medida de proveedores no europeos⁴, lo que aumenta el riesgo de dependencia tecnológica y vulnerabilidad.

Los ciberataques han aumentado significativamente durante la reciente pandemia, habiendo sido dirigidos contra infraestructuras críticas, centros sanitarios, o instalaciones energéticas, como los ciberataques a gran escala que afectaron en Bélgica a la empresa de telecomunicaciones Belnet y al Departamento de Asuntos Internos responsable de la política de inmigración y el orden público en 2021, o el ciberataque contra Ucrania que precedió a la agresión rusa de febrero de 2022⁵. Cabe recordar también en este contexto las palabras del expresidente Juncker de la Comisión Europea en su discurso sobre el estado de la Unión de 2017: «Los ciberataques pueden ser más peligrosos para la estabilidad de las democracias y las economías que las armas y los tanques»⁶.

Los ciberataques también se dirigen contra las instituciones europeas, y en respuesta a este fenómeno creciente, la Comisión presentó en marzo de 2022 una propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a garantizar un elevado nivel

2. Véase la noticia relativa a la publicación del informe, disponible en <https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/> (traducción del autor).
3. Véase a este respecto la información publicada por la Comisión Europea, disponible en el siguiente enlace: <https://digital-strategy.ec.europa.eu/es/policies/internet-things-policy>
4. Véase sobre este punto la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación, Bruselas, 12.9.2018 COM(2018) 630 final 2018/0328 (COD), p. 1.
5. Véase sobre estos ciberataques, entre otros, y. miadzvetskaya, and r.a. wessel, «The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox», *European Papers*, Vol. 7, 2021, N° 1, pp. 413-438, p. 413.
6. Discurso sobre el Estado de la Unión de 2017, disponible en el siguiente enlace: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_17_3165

común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión, basada en el artículo 298 TFUE, relativo a la administración europea «abierta, eficaz e independiente». El Reglamento fue finalmente adoptado el 13 de diciembre de 2023⁷. Por otro lado, la implicación de agentes estatales, como Rusia, China y Corea del Norte, en actividades cibernéticas maliciosas aumenta significativamente la gravedad de la situación⁸.

En este marco, los sujetos de Derecho internacional pueden responder a los ciberataques de distintas maneras con arreglo al Derecho Internacional. En particular, las medidas de autotutela previstas por éste incluyen la retorsión, las contramedidas y la legítima defensa en respuesta a ciberataques. Este libro se centra en la regulación de las contramedidas cibernéticas. No obstante, como ya se ha indicado, se hará también referencia a otras medidas de autotutela, como las represalias y la legítima defensa más brevemente, así como a instituciones que pueden actuar como paliativos o complementos al uso de las contramedidas en este ámbito, caso del estado de necesidad o del principio de debida diligencia. A continuación, se analizará la regulación y práctica de la Unión Europea en dicho supuesto como estudio de caso. Finalmente, se incluyen una serie de consideraciones a modo de conclusión.

II. LAS CONTRAMEDIDAS COMO PARTE DE LA AUTOTUTELA EN EL DERECHO INTERNACIONAL DEL CIBERESPACIO

El Derecho internacional ha carecido tradicionalmente de instituciones que hicieran observar su cumplimiento. En este contexto, los Estados recurrían a diversas formas de autotutela, como las contramedidas, para proteger sus intereses y derechos cuando, a su juicio, un sujeto de Derecho internacional había incumplido sus obligaciones.

Las contramedidas, o represalias como se les denominaba previamente, podían ser incluso armadas hasta 1928, cuando la guerra como instrumento para hacer valer las pretensiones dejó de ser considerada como legítima. Aún entonces, como se desprende de la resolución del asunto *Nauilaa* por un tribunal arbitral en 1928, la prohibición del uso de la fuerza en el ejercicio de represalias no figuraba entre los requisitos para el ejercicio de las contramedidas.

7. Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión, DO L, 2023/2841, 18.12.2023.

8. La declaración del Reino Unido puede consultarse en el siguiente enlace: <https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes>

Estos requisitos sí exigían, de forma similar a como hace el Derecho internacional vigente, cierta proporcionalidad, no debiendo ser excesivas, así como una obligación de intento de arreglo pacífico. Además, su objetivo no debía ser punitivo sino que se centraba en obligar al responsable de una violación de Derecho internacional a reparar la misma⁹.

La creación de las Naciones Unidas en 1945 supondría un cambio significativo en el sistema de autotutela preexistente. En efecto, la constitución de un sistema de seguridad colectiva basado en la prohibición del uso de la fuerza prevista en el artículo 2.4 de la Carta de Naciones Unidas, con la excepción de la legítima defensa *ex* artículo 51 de la misma, excluye el uso de la fuerza en el marco de las contramedidas, las antiguas represalias armadas. Cabe recordar, sin embargo, que las represalias beligerantes sí se aceptan en el contexto de los conflictos armados con arreglo a las condiciones que establece el Derecho internacional consuetudinario aplicable en los conflictos armados internacionales¹⁰.

Además, la Comunidad Internacional se dotó de instituciones para hacer cumplir el nuevo ordenamiento jurídico, y particularmente la prohibición del uso de la fuerza, a través del Consejo de Seguridad. No obstante, como se analiza en esta obra, la autotutela no ha sido erradicada y, de hecho, el Derecho internacional ha regulado las contramedidas con mayor detalle tras la entrada en vigor de la Carta de Naciones Unidas.

Lo anterior es coherente con el hecho de que el cumplimiento del Derecho internacional sigue siendo en gran medida descentralizado, habida cuenta de que las Naciones Unidas no están facultadas para monitorizar y hacer cumplir de manera obligatoria todo el Derecho internacional. Baste a este respecto señalar, por ejemplo, que la jurisdicción de la Corte Internacional de Justicia depende de que los Estados implicados en un asunto la hayan aceptado. A este respecto, ZOLLER definió las contramedidas como «law-enforcement measures which consist of a temporary dispensation

9. Sentencia de 31 de julio de 1928, asunto «Nauliaa», RIAA/RSA, II, pp. 1026-1029.

10. Véase a este respecto la norma 145: Cuando no están prohibidas por el derecho internacional, las represalias bélicas están sujetas a condiciones estrictas. Sobre esta norma puede consultarse el siguiente enlace del Comité Internacional de la Cruz Roja: <https://ihl-databases.icrc.org/es/customary-ihl/v1/rule145>

11. E. Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures*, Dobbs Ferry, N.Y.: Transnational Publishers, Inc., 1984, p. 137, citado por H. Lahmann, *Unilateral*

from complying with the law»¹¹, una definición que subraya la finalidad de hacer cumplir el Derecho que persiguen las contramedidas.

En relación con la terminología, la Comisión de Derecho Internacional ha recomendado la utilización del término «contramedidas» en lugar de represalias o sanciones, aunque reconoce que este último término es utilizado en el marco de Naciones Unidas para referirse a las medidas adoptadas con arreglo al Capítulo VII de la Carta, y ello a pesar de que la Carta utiliza el término «medidas» y no «sanciones». En todo caso, como señala la CDI, al menos desde el laudo arbitral relativo al acuerdo sobre los servicios aéreos de 1978, el término preferido es el de contramedidas, que fue también utilizado en el Proyecto de Artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos, adoptado por la Comisión de Derecho Internacional de 12 de diciembre de 2001 (en adelante también «el Proyecto de artículos de la CDI»)¹².

Las medidas de autotutela, en particular la retorsión, la legítima defensa y las contramedidas constituyen por tanto una parte significativa del Derecho internacional contemporáneo, cuya vigencia ha cobrado especial interés recientemente en el marco de su aplicación al ciberespacio, objeto de estudio de esta obra.

En relación con lo anterior, como indica el Manual de Tallin 2.0, un Estado puede tener derecho a adoptar contramedidas, ya sean de naturaleza cibernética o no, en respuesta al incumplimiento de una obligación de derecho internacional que incumbe a otro Estado¹³. El G7 también subrayó la posibilidad de que los Estados adopten contramedidas cibernéticas¹⁴. En este

Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution, Cambridge University Press, 2020, p. 114.

12. Proyecto de Artículos sobre responsabilidad del estado por hechos internacionalmente ilícitos, adoptado por la CDI en su 53º período de sesiones (A/56/10) y anexoado por la Asamblea General en su Resolución 56/83, de 12 de diciembre de 2001.
13. M. N. Schmitt (editor general), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Regla 20, principio general, p. 112.
14. Declaración del G7 sobre el comportamiento responsable de los Estados en el ciberespacio Lucca, 11 de abril de 2017, p. 2:» Observamos que, en aras de la prevención de conflictos y la solución pacífica de controversias, el derecho internacional también proporciona un marco para las respuestas de los Estados a los actos ilícitos que no equivalen a un ataque armado — estos pueden incluir actividades cibernéticas maliciosas. Entre otras respuestas lícitas, un Estado víctima de un hecho internacionalmente ilícito puede, en determinadas circunstancias, recurrir a contramedidas proporcionadas, incluidas medidas llevadas a cabo a través de las TIC, contra el Estado responsable del hecho ilícito con el fin de hacer que el Estado responsable cumpla con sus obligaciones internacionales».

marco, los próximos capítulos analizan las particularidades y retos específicos que plantea la regulación de las contramedidas en el ciberespacio¹⁵.

15. Proyecto sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, responsabilidad del Estado por hechos internacionalmente ilícitos, Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones Informe de la Comisión de Derecho Internacional, quincuagésimo tercer período de sesiones (23 de abril a 1 de junio y 2 de julio a 10 de agosto de 2001), Suplemento No. 1 (A/53/40), Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones (23 de abril a 1 de junio y 2 de julio a 10 de agosto de 2001), Suplemento núm. 10 (A/56/10), Naciones Unidas, Nueva York, 2001, pp. 1-591, en p. 80.

ESTUDIOS

Este libro analiza la naturaleza y alcance de las contramedidas que pueden adoptar legítimamente los sujetos de Derecho internacional para responder a actividades cibernéticas maliciosas. En particular, el libro examina los requisitos sustantivos y procedimentales que se exigen con arreglo a Derecho internacional para adoptar y mantener contramedidas contra un Estado que ha llevado a cabo un hecho internacionalmente ilícito por medio de la realización de actividades cibernéticas maliciosas. La obra analiza, a la luz de las aportaciones doctrinales y de la práctica internacional, especialmente una de las cuestiones más debatidas en la actualidad en el ámbito de las contramedidas, a saber, la posibilidad de adoptar contramedidas colectivas, teniendo en cuenta los posicionamientos recientes de los Estados, así como de algunas instituciones y órganos de la Unión Europea. El libro analiza asimismo otras medidas de autotutela posibles en el ámbito cibernético, en particular la retorsión y la legítima defensa, con el fin de dar una perspectiva más completa de las opciones de autotutela de las que disponen los Estados. Además, se examina la regulación y práctica recientes de la Unión Europea en materia de contramedidas como estudio de caso, lo que permite ejemplificar algunos de los debates abordados en la obra. Finalmente, se presentan las principales conclusiones del estudio llevado a cabo, en las que se señalan las características más destacadas de las contramedidas cibernéticas, y se apuntan algunos retos presentes y futuros relacionados con su configuración jurídica actual.

ISBN: 978-84-1162-868-6

