neos en cada uno de los capítulos, pero, en su conjunto, se trata de un libro con aportaciones importantes tanto para el proceso de implementación del acuerdo como para documentar y hacer una primera valoración crítica del papel importante y entusiasta de la Unión Europea durante el proceso de negociación y en los primeros siete años de implementación. En suma, se trata de un texto de consulta obligatoria para el caso colombiano y para comparar lo hecho por la Unión Europea en este caso con otros procesos de paz en otras regiones del mundo en los que también la UE tuvo especial relevancia en los años 80 y 90 del siglo. Un texto altamente recomendable

Rafael Grasa
Universidad Autónoma de Barcelona
CIDOB

Piernas López, Juan Jorge. *El Derecho internacional y las contramedidas cibernéticas,* Aranzadi, Madrid, 2024, 168 pp.

La obra cuya valoración iniciamos se centra en uno de los temas más importantes del Derecho internacional de nuestros días, dada la relevancia que en estos últimos tiempos han adquirido las amenazas cibernéticas, tanto en tiempo de paz como de conflicto armado. Y es que hoy en día los Estados se preocupan de poder defenderse no solo frente a ataques cibernéticos en el ámbito privado (bien sea mercantil o de transferencia de tecnología), sino también en caso de guerra, como los conflictos armados entre Rusia y Ucrania o entre Israel y Hamás o Hezbolláh. De ahí que tengamos ejemplos de ataques rusos o de *hackers* (en teoría privados) de esta nacionalidad; o el ejemplo de los *beepers* a los que ha recurrido Israel en su lucha contra Hezbolláh (y es que los atacados desconocían que en la práctica se los estaban comprando al Mossad israelí y, por supuesto, lo que llevaban dentro). Esto revela claramente la complejidad que encierran estos ataques tanto en cuanto a su origen, como en lo que atañe a su contenido, lo que nos permite, además, intuir las dificultades a la hora de adoptar las medidas que puedan legítimamente tomarse a la luz del Derecho internacional para hacer frente a estas actividades.

Pues bien, de todas estas cuestiones trata el autor de la obra que comentamos, y lo hace, según nuestro criterio, de forma clara, completa y precisa, al abordar todos los pormenores que integra el tema, y hacerlo siguiendo un hilo conductor lógico, en el manejo de las fuentes y obras doctrinales relacionadas con la materia, así como de la práctica internacional, que cada día es más importante En su estudio, el autor va desbrozando los requisitos esenciales de las contramedidas que se pueden adoptarse, en el caso de las actividades ciberespaciales, tanto en tiempo de paz como de conflicto armado, siguiendo en su desarrollo una lógica cartesiana y dividiendo la obra en seis partes, que pasamos a analizar.

En la primera de ellas el autor lleva a cabo un estudio sobre las contramedidas como parte de la autotutela en el Derecho internacional relacionado con el ciberespacio, señalando que "los ciberataques representan una creciente amenaza para la seguridad global, así como para los procesos electorales democráticos". Y es que, en efecto, los ciberataques forman parte hoy de la realidad cotidiana. De ahí que, en foros internacionales, como en el Informe de Davos en 2023, se haya establecido "que es probable que se produzca un acontecimiento cibernético catas-

https://doi.org/10.36151/REDI.77.2.35

trófico de gran alcance en los próximos dos años" (p.18). Sin poder pronosticar, claro, con precisión qué pueda suceder en el futuro, lo cierto es que ya hemos tenido ataques cibernéticos importantes durante la pasada pandemia contra ciertas infraestructuras sanitarias críticas, o, en otro contexto, el ciberataque contra Ucrania en 2022. De ahí que algunas personalidades, como un antiguo presidente de la Comisión Europea hayan reconocido que "los ataques cibernéticos pueden ser más peligrosos que las armas y los tanques". Desde este prisma, cabe entender que frente a situaciones de esta índole los Estados y sus instituciones, así como los organismos institucionales internacionales, por ejemplo, los de la Unión Europea, no hayan dudado en protegerse adoptando las "medidas de autotutela" previstas por el Derecho internacional, como la retorsión, las contramedidas e incluso, llegado el caso, la legítima defensa. Estas contramedidas pueden incardinarse, señala el autor, en el marco del Capítulo VII de la Carta de las Naciones Unidas, sin olvidar la precitada legítima defensa, algo que ya se recoge en el Manual de Tallin 2.0 (p.21).

En la Parte II de la obra, la más extensa de la obra, el autor nos ofrece un exhaustivo estudio sobre todo lo relacionado con las contramedidas. El análisis efectuado revela un dominio significativo de esta figura tan controvertida en el Derecho internacional, de ahí que lo primero que lleva a cabo es detenerse sobre el concepto para dilucidar cómo y cuándo se pueden adoptar, partiendo del principio de proporcionalidad. Ya se sabe que el principio de proporcionalidad ha suscitado muchos quebraderos de cabeza a la doctrina internacionalista, al ser un concepto maleable a lora de examinar su aplicabilidad al caso concreto. De ahí las diversas interpretaciones que de él se han hecho. Pero hay, además, otras dos condiciones: la reversibilidad, y la de respetar las obligaciones previstas en el artículo 50 del Proyecto de artículos de la Comisión de Derecho Internacional (pp. 67 y ss.). El autor pasa revista con gran acierto a estas condiciones, cuya complejidad y ramificaciones no son fáciles de cernir, aunque tiene dos buenos maestros en casa, los profesores Cesáreo Gutiérrez Espada y María José Cervell Hortal, cuyos conocimientos del tema habrán permitido al autor abordar con claridad algunas cuestiones sobre las que se ha volcado un relevante sector doctrinal.

En el detallado análisis de estos temas, el autor no se olvida hacer un hueco para examinar la aplicación a las actividades en el ciberespacio de principios de no intervención y el de la debida diligencia. Sabido es que el principio de no intervención ha generado no pocos debates en el Derecho internacional pues constituye un pilar fundamental de su sistema jurídico internacional, pues como ha sido reconocido por la jurisprudencia internacional. Así las cosas, no es extraño que el grupo de expertos que elaborara el Manual de Tallin 2.0 aceptara unánimemente este principio como norma consuetudinaria (p.38), incluyendo los medios cibernéticos, algo de lo que se hace eco el autor. Y es que muchos Estados se han referido a esta cuestión quejándose de intentos de alteración de procesos electorales por medio de actividades cibernéticas maliciosas. Algo similar ocurre con "el principio de la debida diligencia", reconocido también como norma consuetudinaria, y aplicable igualmente a las actividades en el ciberespacio. En este caso, el autor no solo recorre las sendas ya marcadas por el Manual de Tallin 2.0, sino también una amplia práctica en la que los Estados hacen hincapié en que incluso los países por los que transitan los datos están obligados a guardar la debida diligencia.

Tras el análisis efectuado de estas cuestiones, el autor se detiene en un estu-

dio pormenorizado sobre el punto de que "las contramedidas no pueden afectar a ciertas obligaciones internacionales a las que se refiere el artículo 50 del Proyecto de artículos [de la Comisión de Derecho Internacional] sobre responsabilidad del Estado por hechos internacionalmente ilícitos", disposición esta que refleja, asimismo, considera el profesor Piernas López, el Derecho internacional consuetudinario. Continúa su estudio el autor en la Parte III ("Las contramedidas de terceros y contra terceros"), partiendo de la premisa fundamental, de que solo los Estados directamente "lesionados" por un hecho internacionalmente ilícito pueden recurrir a contramedidas contra el "Estado responsable del mismo". Esta afirmación, cierta en principio, puede que, en algunos casos, tenga una difícil aplicación, a causa de la interconexión de las redes a través de las que puede llevarse a cabo los ciberataques, al estar en general en diversos Estados. Por eso no es casualidad que se haya considerado las contramedidas colectivas como "controvertidas", o incluso inaceptables desde el punto de vista jurídico, y a esta solución llegó la Corte Internacional de Justicia en el Asunto de Nicaragua (1986). Sin embargo, esta respuesta deja algunas incógnitas cuando se trata de violaciones de normas *erga omnes* o en caso de obligaciones colectivas por varios Estados (p.102). Esta cuestión ha sido debatida ya en el Manual de Tallin 2.0, que reconoce la legitimidad de contramedidas colectivas. Sin embargo, la práctica estatal sigue siendo, parece controvertida. Entre nosotros, el Prof. Gutiérrez Espada lo tiene muy claro, al haber defendido, con referencia a "la Operación militar espacial de Rusia en Ucrania, la conformidad con el Derecho internacional de las contramedidas colectivas, al menos en el caso de violación de normas imperativas" (p.107).

El autor prosigue su estudio pasando revista, a nuestro juicio con soltura y acierto a las "medidas de autotutela aplicables frente a ciberataques", cuestión presente en la doctrina desde hace algunos años, a la que dedica la Parte IV, iniciando el tema sobre "la retorsión y la legítima defensa". Como se sabe, las medidas de retorsión son actos inamistosos que pueden ser perjudiciales para el Estado en cuestión, pero no son ilícitos así se dan a diario, en particular en el campo de las operaciones cibernéticas. Muy distinto es el caso de la legítima defensa ante ciberamenazas o ciberataques, en la que se requiere un ataque armado previo. A partir de aquí, el autor analiza todos los requisitos necesarios a fin de poder invocar la legítima defensa, que son similares a los conocidos en el Derecho internacional. Una evolución de décadas ha llevado además a aceptar la posibilidad de poder invocar la legítima defensa frente a actores no estatales. Un elemento más específico en el ámbito de las actividades en el ciberespacio que habría que seguir (señala el autor), es el de los efectos o consecuencias, y no el de los medios empleados o el de los objetivos perseguidos. Conviene resaltar que estos aspectos ya figuran en el Manual Tallin 2.0, que el autor precisa con rigor. Así pues, resumiendo, el autor, cuyo libro comentamos, avala la teoría de que nada se opone a que, en caso de ataques cibernéticos, se pueda invocar, dadas todas las circunstancias requeridas, el derecho de la legítima defensa que reconoce el Derecho internacional general y, en particular, el artículo 51 de la Carta de Naciones Unidas.

Por último, en la Parte V el autor se refiere a "las contramedidas en el Derecho de la Unión Europea", advierte que, a fecha de septiembre de 2024, "La Unión no ha publicado una postura común sobre la aplicación del Derecho internacional en el ciberespacio", aunque se conocen las posiciones adoptadas al respecto por sus instituciones (debe en todo caso advertirse que en noviembre de 2024, esa

posición común ya se hizo pública, como el autor del libro que estamos comentando apunta en una publicación ulterior, en prensa en estos momentos). En esencia, la Unión Europea ha ido adoptando en lo que se ha denominado el "EU Cyber Security Package" en torno a tres objetivos: reforzar la resiliencia a los ciberataques, crear una ciber disuasión y fortalecer la cooperación en la materia. Desde este prisma, el autor expone con soltura el posicionamiento de las distintas instituciones, recalcando los problemas que surgen en el caso de los ataques híbridos, tan de moda hoy (casos de Rusia, y en menor medida quizás, también con China).

El profesor Piernas López cierra, el que nos parece, su exitoso estudio con doce conclusiones recogidas en la Parte VI, reconociendo que las medidas cibernéticas son lícitas siempre que se respeten los requisitos exigidos por el Derecho internacional, como es el de la proporcionalidad. El autor señala, además, que de la práctica estatal se deduce que los Estados no dan la misma importancia que la Comisión de Derecho Internacional o la jurisprudencia a la cuestión de la reversibilidad de las contramedidas, ya que pocos Estados hacen referencia a esta cuestión. Otro problema importante es que tanto la doctrina como la práctica estatal avalan la prohibición de la amenaza y del uso de la fuerza, sobre todo este último. Conviene apuntar, igualmente, que algunos de los requisitos de las contramedidas no aparecen en las posiciones estatales sobre la aplicación del Derecho internacional al ciberespacio. Otra diferencia existente atañe a los requisitos "procesales" de las contramedidas, ya que varios Estados han manifestado sus dudas respecto a su aplicación al ciberespacio Subsisten dudas también respecto de la obligación de la notificación ante cualquier contramedida. Sin embargo, sí que ha sido reconocida, tras la crisis ucraniana, la conformidad de las contramedidas colectivas sobre todo en el caso de violación de normas imperativas. También se menciona que muchos Estados han avalado la adopción de medidas de autotutela distintas a las contramedidas para responder a ciberataques. Es más, los Estados podrían invocar incluso el estado de necesidad en esta materia. Y, por último, se afirma que la Unión Europea ha defendido la aplicabilidad de todo el Derecho Internacional al ciberespacio, lo que podría favorecer en este ámbito el desarrollo progresivo del Derecho internacional.

Escrito lo escrito, solo nos queda felicitar al autor por habernos aclarado aspectos particularmente complejos o en discusión del Derecho internacional aplicable al ciberespacio, de forma que este trabajo será, sin duda (en opinión, al menos, de quien firma estas palabras), un punto de referencia obligado para la doctrina internacionalista e, incluso, para la práctica estatal.

Romualdo Bermejo García
Universidad de León

Pla Almendros, Rosa, *La solución extrajudicial de disputas transfronterizas en el reglamento europeo de servicios digitales*, Colex, A Coruña, 2025, 256 pp.

Lograr una protección eficaz del usuario de servicios digitales, potenciación de los medios de solución extrajudicial en línea, adopción de una regulación europea coherente y efectiva de las plataformas en línea y dificultades para abordar el tratamiento e impugnación de las decisiones de moderación de con-

https://doi.org/10.36151/REDI.77.2.36