DOI: 10.15581/010.40.760-763

CERVELL HORTAL, María José y PIERNAS LÓPEZ, Jorge Juan (dirs.)

Hacia una regulación internacional para el ciberespacio

Aranzadi, Cizur Menor (Navarra) 2023, 378 pp.

Parece indiscutible que el nuevo espacio global común, conocido como ciberespacio, está sometido al Derecho internacional, como ya lo afirmó la Asamblea General de las Naciones Unidas en 2019 (y anteriormente la OTAN), aunque resulta más controvertido saber qué áreas concretas del ordenamiento internacional se aplican directamente a este ámbito. También puede afirmarse al respecto que existe un consenso generalizado entre la doctrina –que ha llegado a cristalizar en la práctica de algunos Estados– de que el Derecho internacional resulta aplicable a este espacio. No obstante, si bien puede sostenerse que existen ya normas aplicables a las actividades desarrolladas en el ciberespacio, convendría que dichas normas fueran más precisas y adaptadas a las complejas y específicas características que presenta el marco en que aquéllas deben aplicarse. El hecho de que no exista un tratado internacional general sobre el ciberespacio, ni que se le espere en el futuro más inmediato, así como las dificultades manifestadas por los Estados para llegar a acuerdos consensuados en esta materia, hace más que conveniente tratar de buscar alternativas al marco regulatorio formal, a través de iniciativas no estatales, grupos de trabajo especializados... que, sin ser vinculantes, se conviertan en un marco de referencia para la acción de los Estados en este ámbito. Sin embargo, ello no debe impedir el hecho de

que se explore y, en la medida de lo posible, se impulse desde los sectores pertinentes, la progresiva adopción de una normativa jurídica más precisa y adecuada. En este sentido, comparto la propuesta realizada por algunos autores de que podría aplicarse al ciberespacio un *odos* similar al seguido por la comunidad internacional para regular las actividades de los Estados en el espacio ultraterrestre. Sin duda, el camino estará plagado de dificultades, pero daría más certeza jurídica a la regulación internacional de un ámbito que por la carencia de fronteras físicas se ha convertido en una preocupación prioritaria para los Estados.

El libro objeto de la presente recensión es resultado del proyecto de investigación «La búsqueda de una regulación internacional para las actividades cibernéticas ¿una ineludible necesidad?», en el marco de los programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico («Retos de la Sociedad»), que incorpora un nutrido y variado grupo de expertos y profesores procedentes de las Universidades de Murcia, Navarra y Lleida, siendo los Investigadores principales y directores del presente libro, la profesora María José Cervell Hortal, Catedrática de Derecho Internacional Público y Juan Jorge Piernas López, Profesor Titular, ambos de la Universidad de Murcia. El resultado es un excelente y poliédrico trabajo de investigación que aporta reflexiones de gran interés y actualidad sobre las nuevas dimensiones que presenta la regulación internacional del ciberespacio en el momento presente, así como las nuevas vías que se abren de cara al futuro

La obra se estructura en dos grandes partes que se dedican respectivamente a los problemas concretos del ciberespacio desde la perspectiva del Derecho internacional, y al análisis de otras aproximaciones regulatorias desde la perspectiva europea y española. Con un enfoque cuidadosamente equilibrado entre ambas, la Primera Parte (pp. 25-253), incorpora un total de siete capítulos y analiza cuestiones de gran novedad como el uso de la fuerza y la legítima defensa en el ciberespacio, introduciendo un análisis muy novedoso de conceptos aplicados a este ámbito como la soberanía o la noción de combatiente o la aplicación de principios como el de continuidad de la acción o el de distinción (capítulo 1: Enrique Cubeiro Cabello, director de ciberseguridad de GHENOVA); la protección ofrecida por el Derecho internacional frente a los ciberataques contra las infraestructuras críticas de los Estados, dado que si se producen en el marco de un conflicto armado, ya sea interno o internacional, se aplicarán las normas y los principios generales del DIH, en particular el de humanidad, necesidad y proporcionalidad (capítulo 2: prof. Andrea Cocchini. Universidad de Navarra); la imputación al Estado de la responsabilidad internacional por actividades cibernéticas malintencionadas que, en aplicación del «Manual de Tallín», elaborado por un Grupo Internacional de Expertos en 2013 creado a raíz de los ciberataques sufridos por Estonia en 2007, establece una serie de reglas que reflejan el Derecho internacional consuetudinario aplicable a los conflictos en el ciberespacio, recogiendo en particular los principios esenciales del Derecho internacional de la responsabilidad en vigor (capítulo 3: prof. Cesáreo Gutiérrez Espada. Universidad de Murcia); las normas no vinculantes, en particular de *soft law*, como alternativa a la dificultad existente para adoptar normas jurídicas vinculantes que regulen el ciberespacio, y que lleguen a convertirse en guías de acción para los Estados, en particular el citado Manual de Tallín y otras iniciativas, especialmente las derivadas del Grupo de Expertos Gubernamentales de Naciones Unidas (capítulo 4: prof. María José Cervell Hortal. Universidad de Murcia); el uso del ciberespacio para el control de armamento químico, y en particular la aplicabi-

lidad de la tecnología *blockchain* –en especial a través del prototipo MATCH– para fortalecer los controles transfronterizos de armamento químico a partir del intercambio de información entre Estados con el objetivo último de fortalecer la seguridad internacional (capítulo 5: prof. Mónica Chinchilla Adell. Universidad de Navarra)

Si los cinco primeros capítulos de la Primera Parte se dedican al análisis de aquellas cuestiones que afectan más directamente al Estado, los dos capítulos siguientes se destinan a aquellas que afectan de forma más directa al individuo. En este sentido, se incorpora la cuestión novedosa de la responsabilidad penal internacional en el ciberespacio, en particular si los ciberataques pueden llegar a convertirse en un crimen de guerra, y en cuanto tal, ser su autor penalmente responsable ante la Corte Penal Internacional o, en su caso, ante las jurisdicciones estatales de acuerdo con la obligación de los Estados de investigar y enjuiciar los crímenes de guerra (capítulo 6: prof. Irene Vázquez Serrano. Universidad de Murcia); y finalmente, la cuestión del ciberespacio y los derechos humanos de las mujeres en el orden jurídico internacional que incluye la violencia (*online*) de género como una forma de discriminación contra las mujeres y las niñas, o el ciberespacio y la libertad de expresión desde la perspectiva de género (capítulo 7: prof. Dorothy Estrada Tanck. Universidad de Murcia).

La Segunda Parte del libro (págs. 257-378) incorpora cuatro capítulos dedicados a analizar las diferentes iniciativas europeas (también desde la perspectiva del Derecho penal español) en este ámbito. A tal efecto, se incluyen una serie de materias como la necesidad de mejorar la ciberdefensa como política europea, en la medida en que ésta exhibe importantes carencias a pesar de la adopción de una serie de propuestas políticas que tienen como objetivo la adaptación progresiva a las capacidades de defensa en el marco de la OTAN y de la UE (capítulo 8: prof. Eimys Ortiz. Universidad de Lleida); la protección de los derechos y valores fundamentales de la Unión Europea en el ámbito de la política de ciberseguridad, tanto en su dimensión interna, en particular el espacio de libertad, seguridad, justicia y el mercado interior, como en su dimensión externa, especialmente la adopción de acuerdos internacionales con terceros en este ámbito, identificándose al respecto una serie de derechos fundamentales que pueden verse afectados en el marco de la ciberseguridad (capítulo 9: prof. Juan Jorge Piernas López. Universidad de Murcia); la cooperación de la Unión Europea para la construcción de la ciberseguridad en América Latina y el Caribe, dada la escasa implantación de los sistemas de ciberseguridad en este ámbito geográfico, a pesar de los esfuerzos concertados de los Estados de la región para dotarse de las necesarias cibercapacidades, siendo la cooperación europea fundamental para implementar compromisos bilaterales, regionales y birregionales en el marco de la Asociación Estratégica Birregional UE-ALC (capítulo 10: prof. Eugenia López-Jacoíste Díaz. Universidad de Navarra); y finalmente, y desde la perspectiva del Derecho penal español, los problemas y las reformas legislativas que han llevado al legislador español a adoptar una serie de medidas ante la proliferación de delitos en el ciberespacio y las consecuencias nefastas que éstos producen (capítulo 11: prof. Samuel Rodríguez Ferrández. Universidad de Murcia).

Para concluir, debe subrayarse la pertinencia de una obra de estas características en el momento presente caracterizado por una extrema volatilidad e inestabilidad, por lo que debemos congratularnos por su aparición y felicitar a sus directores por esta iniciativa, y a los coautores por contribuir a materializarla. Sin lugar a dudas, la lectura de esta obra resulta obligada no sólo para aquellos que se acerquen a un concepto tan poliédrico y com-

plejo como el de la regulación internacional del ciberespacio y sus múltiples consecuencias, sino también para aquellos estudiosos del Derecho internacional que desean estar atentos a su evolución y a sus múltiples manifestaciones. En definitiva, nos encontramos ante una obra imprescindible para quienes se aproximen al estudio de un tema que plantea innumerables desafíos en el momento presente y que, como tal, exige una respuesta adecuada del ordenamiento jurídico internacional.

Antonio BLANC ALTEMIR
Catedrático de Derecho Internacional Público
y Relaciones Internacionales
Universidad de Lleida