guiendo la autora tres bloques: a) situaciones invocadas y que la Guía trata de manera exhaustiva, como la violencia intrafamiliar (con respecto a la que se propone la modificación del párrafo 58 de la Guía), el encarcelamiento del sustractor, la separación de los hermanos y las desventajas económicas; b) situaciones invocadas pero excluidas de la Guía, para las que la autora distingue entre las que han sido consideradas improcedentes y procedentes por los tribunales; c) situaciones que en la Guía han sido tratadas de manera breve y que la autora expone que merecen un análisis más profundo, como son los casos de países en guerra y los casos de abusos sexuales.

La segunda excepción, con la que finaliza la obra, es la oposición del menor a su restitución, prevista en el art. 13(2) del Convenio. Destaca el examen de dos cuestiones clave, cuyo estudio se acompaña igualmente de un detallado análisis jurisprudencial: a) la determinación de la edad y grado de madurez, y b) la valoración de la oposición. Al respecto, se distingue acertadamente entre casos en los que los tribunales consideraron que el menor no contaba con suficiente edad y grado de madurez; y casos en los que, a pesar de una edad y grado de madurez suficiente, la opinión del menor no fue decisiva por diversos factores.

En conclusión, como habíamos adelantado, resulta totalmente justificada la investigación que la autora ha desarrollado sobre el Convenio de La Haya de 1980, puesto que se hace un profundo análisis de aspectos clave del Convenio y, efectivamente, se aportan *soluciones* a los problemas de aplicación.

Celia M. Caamiña Domínguez
Universidad Carlos III de Madrid

Cervel Hortall, Mª José y Piernas López, Juan Jorge (dirs.), *Hacia una regulación internacional para el ciberespacio*, Aranzadi, 2023, 378 pp.

Cuando Max Huber afirmó hace casi un siglo en el laudo arbitral de 4 de abril de 1928 (Isla de Palmas) el carácter exclusivo de la soberanía territorial, resultaba imposible concebir la noción de espacio sin territorio… físico. La clave del desarrollo del Derecho internacional en el orden westphaliano se encontraba en dirimir en qué partes del territorio el Estado ejercía sus poderes soberanos y, eventualmente, qué régimen resultaba aplicable a las actividades desarrolladas en los territorios más allá de la jurisdicción del mismo.

Cuando aún estamos buscando respuestas para las actividades que se realiza(rá)n en ciertos espacios, como la minería espacial, el paradigma de análisis ha cambiado. El ciberespacio se configura como un "espacio no espacial", si se permite la *boutade*, en el que los Estados ejercen competencias. Tales actividades están, deben estar, sujetas de una u otra forma al imperio de la ley, a la regulación jurídica. El Derecho abomina del vacío. El libro que comentamos construye, a través de un conjunto de ensayos singulares, una aproximación imprescindible a la necesidad de regulación internacional del ciberespacio. Como obra colectiva, los directores han escogido un enfoque de coloreado: han inyectado tintura en elementos diversos de un panorama de Derecho internacional para así exponer los vacíos regulatorios, o la posibilidad de proyectar el derecho existente sobre la nueva realidad del no-espacio ciberespacio. huyendo así del *horror vacui* legal.

Una primera característica de esta obra deriva de su estructura en dos par-

tes. Combina una selección de temas relativos a la regulación internacional, en el sentido de universal, en su primera parte (*Primera parte. Una regulación para el ciberespacio desde el Derecho Internacional*, pp. 21-253), con un análisis regional europeo que desciende hasta algún elemento específico del ordenamiento español (*Segunda parte. Otras aproximaciones regulatorias: la Unión Europea y España*, pp. 255-378).

Dentro de la primera parte dedicado al análisis de Derecho internacional (universal) se prueba y testimonia la evolución de los fundamentos clásicos de nuestra doctrina internacionalista. Frente a la lógica devoradora del Estado como clave interpretativa del Derecho internacional, los directores han dividido las aportaciones en dos subpartes. Por un lado, analizan las *Respuestas (y silencios) normativos de los Estados en el ciberespacio*, a lo largo de cinco capítulos. Por otro lado, y siendo predominante esta visión interestatal, reserva una subparte específica y autónoma a *La protección del individuo en el ciberespacio*, con dos capítulos. Sin duda, la protección del individuo es competencia estatal, la posible canalización de tal protección a través de mecanismos de derechos humanos existentes es también emanación de la soberanía (todo sistema internacional de protección es eminentemente subsidiario). Por ello, quiero resaltar el carácter no aleatorio de la estructura y la puesta en valor de una declaración de principios sobre una concepción del orden jurídico internacional, más allá del Estado y las relaciones interestatales como elemento definitorio del Derecho internacional y el estudio de sus límites contemporáneos.

El primer capítulo, titulado *La legítima defensa: ¿Un derecho fallido en el ciberespacio?* (pp. 25-53), está firmado por Enrique Cubeiro Cabello. La colaboración de un profesional, capitán de navío en la reserva, y Director de Ciberseguridad de una empresa dedicada a sectores como el Naval y Defensa, la Energía e Industria o la Transformación Digital e Infraestructuras, enriquece sin duda la obra. Como contribución inicial, y a partir de la noción de legítima defensa, identifica e introduce un amplio abanico de cuestiones sobre las que se irá ahondando en capítulos sucesivos: el concepto de soberanía en el ciberespacio, la responsabilidad del Estado, principios generales del derecho como el de distinción y el de proporcionalidad, propios del Derecho internacional humanitario, o cuestiones más globales como la "asimetría legal".

En el segundo capítulo, el profesor Andrea Cochini centra la problemática de la aplicación del Derecho Internacional Humanitario al fenómeno del ataque cibernético, no cinético, aunque en muchos casos incardinado en operaciones armadas más amplias, con ejemplos recientes tomados de la guerra ruso-ucraniana (*Los ciberataques contra las infraestructuras críticas de los Estados: ¿Cómo nos protege el Derecho internacional?*, pp. 55-91).

El profesor Cesáreo Gutiérrez Espada presenta un análisis de los problemas de atribución en términos de responsabilidad internacional en el capítulo tercero (*Sobre la imputación (o atribución) al Estado de la responsabilidad internacional por actividades cibernéticas malintencionadas*, pp. 93-121). Junto al análisis de la teoría clásica interestatal, que realiza a través de los artículos sobre responsabilidad de los Estados por hecho ilícito, elaborados por la CDI y adoptados por la Asamblea General, y su aplicación jurisprudencial, introduce el examen de las normas de atribución del Manual de Tallin 2.0. Define este texto como un "referente sin duda en el contexto de la situación de incertidumbre que generan las actividades en y desde el ciberespacio" (p. 106) y que considera "pretenden reflejar el Derecho internacional consue-

tudinario aplicable a los conflictos en el ciberespacio" (p. 107), estableciendo un paralelismo con la propia naturaleza legal de los artículos sobre responsabilidad. Y hasta aquí puedo escribir: porque su capítulo no solo debe ser leído, sino estudiado.

La profesora María José Cervell, co-directora de la obra, firma el capítulo cuarto con un análisis sobre la preponderancia —o no— de normas de soft law en el sector del ciberespacio *(¿Un* soft law *para el ciberespacio? (De las normas no vinculantes y otras iniciativas)*, pp. 123-158). Su punto de partida es la aplicación del Derecho internacional "general" al ciberespacio, aunque sus características especiales "dificultan la aplicación de los parámetros tradicionales a los problemas más recientes" (p. 127). Ello le lleva a indagar en los distintos esfuerzos normativos desarrollados y su naturaleza jurídica.

El último de los capítulos de este bloque centrado en las relaciones interestatales en el marco de la dimensión universal aborda *El uso del ciberespacio para el control de armamento químico. El estatus jurídico de la tecnología blockchain y sus beneficios* (pp. 159-194). Mónica Chinchilla Adell nos presenta aquí una confluencia —que califica de insospechada (p. 173)— entre dos sectores específicos: la tecnología *blockchain*, como manifestación de actividad ciberespacial "pacífica", y el control de armas químicas como área específica del Derecho internacional que, aun encontrándose fuera del ámbito específicamente regulatorio del conflicto armado, está en el corazón de la paz y seguridad internacionales.

A lo largo de los cinco capítulos que giran sobre las relaciones interestatales se entrecruzan tres líneas discusión de clave y constante: la naturaleza jurídica de las normas específicas relativas a actividades en el ciberespacio y la aplicabilidad de normas generales (primarias o secundarias) de otros subsectores; la regulación del uso de la fuerza en conexión con el ciberespacio; y, la responsabilidad eventual del Estado por hecho ilícito mediante comportamiento atribuibles al mismo realizados en el ciberespacio.

Pasando a la dimensión humana, y en perspectiva universal, esta obra nos presenta dos escenarios diferentes desde los que abordar el papel protector del Derecho internacional en relación con el individuo en el ciberespacio. El capítulo firmado por la profesora Irene Vázquez Serrano con el título *La responsabilidad penal internacional en el ciberespacio: ¿hacia el cibercrimen de guerra?* (pp. 197-225) cierra el círculo de la relación entre ciberespacio y el *Ius in bello*, ya presente en capítulos previos. La diversidad de los problemas analizados (ciberataques como crímenes no cinéticos, ciber actores no estatales y responsabilidad internacional penal) llevan a la autora a discutir la necesidad de una "nueva jurisdicción y una nueva competencia de la Corte Penal Internacional" (pp. 217-220).

En esa estructura clásica de Derecho de la guerra y Derecho de la paz, un subsiguiente capítulo afronta los derechos humanos en el ciberespacio. Como no podía ser de otra forma, la profesora Dorothy Estrada Tanck se concentra en *Ciberespacio y derechos humanos de las mujeres en el orden jurídico internacional: discriminación, violencia de género y espacios de igualdad* (pp. 227-253), ofreciendo una visión constructiva, positiva y progresista. Frente a los capítulos previos en los que el ciberespacio se constituía como escenario de posibles amenazas a la sociedad internacional contemporánea, la profesora Estrada Tanck nos abre la mente a las posibilidades que el ciberespacio y la tecnología ofrecen a la perspectiva de género y, en general, al enfoque basado en derechos humanos.

La segunda parte de la obra, sobre dimensiones regionales e internas de la

regulación del ciberespacio (*Otras aproximaciones regulatorias: la Unión Europea y España*, pp. 255-378), se desarrolla a través de cuatro capítulos. Los tres primeros capítulos exploran diversos aspectos de la política europea en relación con ciberespacio.

La profesora Eimys Ortiz Hernández, en su capítulo titulado *La necesidad de mejorar la ciberdefensa como política europea* (pp. 257-283) estudia la dimensión de cooperación de la política exterior y de seguridad común. Desde tal perspectiva, resulta relevante el papel de la ciberdefensa el cual se visibiliza en aspectos como la inclusión de la ciberdefensa en la cooperación estructurada permanente y el Fondo Europeo de Defensa: inversión en capacidades, coordinación frente a los ataques y prevención de los mismos resultan todos aspectos claves desarrollados con esmero por la autora.

El profesor —y co-coordinador de la obra— Juan Jorge Piernas López aborda la perspectiva clave de la protección de derechos fundamentales en relación con ciberseguridad de forma sistemática y comprehensiva. En sus páginas encontramos el análisis tanto en su vertiente exterior como interior. En esta última aborda aspectos tan diversos como la citada protección a través de la realización del Espacio de Libertad, Seguridad y Justicia (incluyendo la normativa específica sobre cibercriminalidad) y del mercado interior (*La política de ciberseguridad de la Unión Europea y los derechos fundamentales reconocidos por la Unión*, pp. 285-316).

Estratégicamente situado, el capítulo firmado por la profesora Eugenia López Jacoíste traza un puente intercontinental para analizar en términos de oportunidad la cooperación entre la Unión Europea y América Latina en materia de ciberseguridad (*La cooperación de la Unión Europea para la construcción de la ciberseguridad en América Latina y Caribe*, pp. 317-353), concretando las agendas y proyectos conjuntos en relación con ciberseguridad y ciberdelincuencia, en el marco de iniciativas como la estrategia *Global Gateway* o la Alianza Digital UE-ALC, ambas de 2021, o la más reciente (2023) nueva agenda para las relaciones entre la UE, América Latina y Caribe.

La obra concluye con último capítulo, en ing,lés, relativo a la regulación penal nacional en España en relación con ciberseguridad firmado por Samuel Rodríguez Ferrández (*Cybersecurity: legal criminal aspects in Spain*, pp. 355-378). Aun cuando es una aportación interesante y valiosa, es difícil entender la opción idiomática. La presión, probablemente, de los procesos de acreditación nacional lo expliquen. Dejándome llevar por mis propios intereses en el tema, este trabajo quizás podría haber valorado la ratificación española de la Convención de Budapest sobre cibercriminalidad, de 23 de noviembre de 2001, en vigor internacionalmente desde el 1 de julio de 2004 (ETS No. 185, con 67 Estados parte, de los cuales 22 no son miembros del Consejo de Europa). En ese mismo sentido, habría sido interesante una valoración del acomodo entre la tipificación interna actual y la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, (DO L 218 de 14.8.2013), que como el anterior Convenio Europa aparecen, en cambio, convenientemente referenciados en el capítulo del Prof. Piernas López. Igualmente, interesante hubiera sido una visión penalista sobre los trabajos en curso en Naciones Unidas para una futura convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos a la luz de la tipificación española.

Las obras colectivas pueden examinarse como fruto característico de nuestro sistema investigador: en primer lugar, permiten visibilizar los resultados de la investigación colectiva; en segundo lugar, estimulan la convivencia entre investigadores experimentados y aquellos más jóvenes; y, en tercer lugar, prueban la capacidad de liderazgo —como ahora gustan las agencias evaluadoras denominarlo— de sus directores.

Bajo esta triple premisa, esta monografía constituye un magnífico ejemplo de las tres dimensiones. Con el título *Hacia una regulación internacional para el ciberespacio* este libro consolida el trabajo desarrollado en el marco del proyecto de investigación "La búsqueda de una regulación internacional para las actividades cibernéticas, ¿una ineludible necesidad?", proyecto financiado por la Agencia estatal de investigación entre 2021 y 2024. Asimismo, los directores —profesores en distintos momentos de sus carreras académicas— han consolidado una monografía en la que se integran investigadores en muy diferentes momentos de sus trayectorias investigadoras, sin caer en la ordenación jerárquica fácil, pero vacua en términos de contenidos, a la hora de ordenar los capítulos. Por último, estos mismos directores han sabido con acierto proponer una obra con bibliografías finales en cada capítulo, de gran ayuda para quien buscar acercarse a temas específicos. Por su parte, los autores han mostrado un apego a la realidad, muy necesario cuando se afrontan temas novedosos. En particular, Andrea Cocchini, Gutiérrez Espada, Estrada Tanck, Piernas López, entre otros, provisionan sus capítulos de datos, casos y ejemplos significados de la realidad que analizan. Ello ameniza la lectura y hace más comprensible la materia. Si algo queda por comentar, es la ausencia de una "parte general" antes de las especificidades: conceptos como el del propio ciberespacio, que el profesor Gutiérrez Espada analiza, no se introducen hasta las páginas 103-106 de la obra.

Sin duda, no se ha buscado una obra conceptual sobre la teoría del (no) territorio ciberespacio, ni sobre las manifestaciones y limitaciones de la soberanía en el mismo, sino de manera indirecta. Esta monografía sobresale por la diversidad de planteamientos y riqueza de temas desde los que una nueva realidad puede ser objeto de estudio. Y en ello mismo reside su gran aportación. No por ello dejamos de animar a los directores a que planifiquen ya esa nueva obra, complementaria de esta, y de la cual la rica doctrina de habla hispana carece.

Eulalia W. Petit de Gabriel
Universidad de Sevilla

Chinchilla Adell, Mónica, *El régimen jurídico internacional para la no proliferación de las armas biológicas y químicas*, Cizur Menor, Aranzadi, 2023, 316 pp.

La amenaza química y biológica, en su dimensión estatal y, de forma especial, por parte de actores no estatales, es objeto de una creciente preocupación internacional constituyendo, además, un importante desafío a la seguridad. Así lo ha reconocido, por lo que se refiere al ámbito químico, la Organización para la Prohibición de las Armas Químicas (OPAQ), encargada de la aplicación de la Convención sobre las Armas Químicas (CAQ), el primer acuerdo multilateral de desarme a nivel mundial, adoptado en 1992, que contempla la eliminación de