
CERVELL HORTAL, María José (dir.)

Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio

Thomson Reuters Aranzadi, Cizur Menor, 2020, 341 pp.

Las nuevas tecnologías se han convertido en un nuevo universo en el que la robótica va cubriendo espacios donde se trastoca el protagonismo de las personas que se refugian detrás de los algoritmos. Se trata de un cambio radical de percepciones y de transformación de los escenarios que ha modificado los comportamientos y el resultado de las acciones humanas. En este contexto, las nuevas corrientes tecnológicas van a influir necesariamente en el uso de la fuerza con la introducción de nuevos modelos de ingenios bélicos. El trabajo coral que realiza la profesora Cervell Hortal presenta el encomiable esfuerzo capaz de aglutinar a diez expertos de cinco universidades con la capacidad y el conocimiento de abordar temas de importante actualidad como es el caso de los drones, las armas autónomas y el ciberespacio. La impecable estructura de la obra, que se divide en estos tres ítems señalados, facilita al lector un acercamiento ordenado al conocimiento del modo en el que las nuevas tecnologías se han integrado en las estrategias del uso de la fuerza en la comunidad internacional.

En la primera parte, el análisis de los drones a la luz del *ius ad bellum* a cargo de Bermejo García resulta sumamente sugestiva dado que en un detallado examen concluye que «el recurso a los drones para llevar a cabo operaciones militares es completamente legal, los Estados que recurran a la fuerza al amparo de una decisión del Consejo de Seguridad adoptada en el ámbito del capítulo VII, no sería necesario que el uso de los drones estuviera recogido *expressis verbis* en dicha decisión» (p. 60). Por lo que respecta al empleo de drones armados desde la perspectiva del derecho internacional humanitario y del derecho internacional de los derechos humano, López-Jacoiste Díaz, reconoce que el desarrollo tec-

nológico de las últimas décadas ha favorecido la modernización de las fuerzas armadas y, por tanto, ha modificado sustancialmente los modos de conducir las hostilidades. Si bien los drones *per se* no son armas prohibidas, las cuestiones que plantea el empleo de drones armados se mueven dentro de un «marco jurídico imperfecto», no obstante, como señala su autora «tanto el derecho internacional humanitario como el derecho internacional de los derechos humanos contemplan normas, criterios y principios suficientes como para dar una respuesta conforme al Derecho vigente a los retos que plantean las nuevas tecnologías en el transcurso de las guerras» (p. 104). Por su parte, Ortiz Hernández, al estudiar la improbable consecución de la Unión Europea de una convergencia de mínimos en materia de drones armados, considera que la Unión ha realizado aún pocos avances y que el horizonte de la convergencia queda todavía lejos dado que esta materia se encuentra intrínsecamente relacionada con la seguridad nacional por lo que «llevará un tiempo a que los Estados miembros opten por una posición común» (p. 128).

En la segunda parte de la estructura temática de la obra, dedicada a las Armas Autónomas, Cervell Hortal analiza su regulación y responsabilidad como claves de su estudio, dado que el Derecho Internacional no autoriza ni prohíbe el uso de un arma concreta, lo cual resulta perturbador en una época de avances tecnológicos sorprendentes con armas que parecen distópicas. No obstante, como apunta su autora «los Estados no tienen un derecho ilimitado de elección de los medios y métodos de combate con un conflicto armado y que el Derecho Internacional contempla prohibiciones específicas» (p. 135). Sin embargo, existe la posibilidad de

emplear en combate armamento teledirigido o semi-autónomo y el siguiente paso será el funcionamiento totalmente autónomo de un arma mediante la aplicación de la inteligencia artificial. Ante esta cuestión, resulta aún hipotético que los Estados firmasen un tratado que prohíba este tipo de armas, por lo cual, «lo más factible sería, quizás y al menos de momento, una solución a nivel político, con la que los Estados, por ser la más flexible, se mostrarán menos recelosos» (p. 160). Cuestión que no debería dilatarse puesto que se trata de una tecnología que se está desarrollando y frente a la cual convendría elaborar un «código de conducta, compromisos de cooperación y transparencia, nombramiento de una comisión encargada de dictaminar los requisitos mínimos que tendría que reunir un arma autónoma para ser legal o que pudiera vigilar el cumplimiento de unas normas mínimas de funcionamiento» (p. 161). Continuando con el esquema de estudio, el siguiente trabajo a cargo de Vázquez Serrano se dedica a analizar los retos y dilemas que presentan las armas autónomas ante el Derecho Internacional Humanitario. Si bien, la creación de armas completamente autónomas no se ha plasmado aún, «se hace necesaria la presencia de un 'regulador ético' (...) esto es selección de objetivos y ataque (...) que le permitan cumplir con los límites claros que establece el Derecho Internacional Humanitario» (p. 190). Por lo que respecta a la responsabilidad internacional en el uso de las armas autónomas, Estrada Tanck, recomienda que el reto actual estaría en utilizar los principios y las normas del Derecho Internacional Humanitario y del Derecho Internacional de los Derechos Humanos e incluso en materia de responsabilidad «no debemos dejar de lado el derecho internacional penal –compatible y combinable con la responsabilidad del Estado, las organizaciones internacionales, u otros autores de ser aplicable– pues con la eventual creación de los robots asesinos se abriría la puerta a reflexionar sobre la equiparación del robot a una persona para efectos de responsabilidad» (p. 220).

La tercera parte de la obra, dedicada al Ciberespacio, se abre con las reflexiones de Gutiérrez Espada cuando se pregunta sobre si existe en la actualidad un derecho aplicable a las actividades en el ciberespacio. Surge en este contexto un nuevo ámbito de aplicación del derecho en este llamado el «quinto elemento» teniendo en cuenta al territorio, el mar, el aire, el espacio ultraterrestre y que el autor con acierto califica como el «sexto elemento» si se tiene en cuenta también a los espacios polares. Por otra parte, el ciberespacio al no ser un espacio físico, sino una realidad virtual que se articula con el enjambre de los ordenadores, servidores y redes del mundo ha generado un ámbito de ilegalidad a través del cibercrimen, del ciberterrorismo y la ciberguerra en su uso malsano. Si bien, la ciberguerra es la amenaza más importante, que como principal arma utiliza artificios cibernéticos, tales como los virus informáticos, de tal modo que se les ha bautizado como «armas de interrupción masiva» por el descalabro que pueden provocar colapsando los sistemas de vida de una población. En este sentido, destaca su autor que el Manual de Tallinn 2.0, sobre la aplicación del Derecho Internacional al ciberespacio, surge en el contexto de la incertidumbre que generan las nuevas formas cibernéticas de la guerra. En efecto, los ataques a Estonia en 2007 dieron lugar a la reacción de la OTAN que estableció en Tallin, capital de Estonia, el Centro de Excelencia para la Ciberdefensa Cooperativa con la creación de un Grupo Internacional de Expertos en Defensa, Seguridad y Derecho Internacional, aplicable al ciberespacio como teatro de hostilidades. Estos modelos innovadores determinan nuevos escenarios para el desarrollo de los conflictos y actualmente no existe tratado internacional que regule con carácter general el uso del ciberespacio como ámbito de hostilidades en una guerra o al uso de la fuerza. Sin embargo, Gutiérrez Espada considera que «el Derecho Internacional existente resulta, sin duda, aplicable a este nuevo escenario» y agrega que «personalmente, no encuentro razones para pensar

que el Derecho Internacional en vigor no pueda aplicarse a las actividades humanas en el ciberespacio, en particular aquellas de sus normas que se refieren al uso de la fuerza armada y a la responsabilidad internacional que de su empleo ilegal (no conforme, por tanto, con el Derecho Internacional) resultase» (p. 239). Al punto que, por su parte, Cocchini se pregunta si es necesario elaborar un nuevo *ius ad bellum* frente al uso de la (ciber) fuerza y a los ciberataques (armados), por lo que destaca que «una acción cibernética ofensiva puede calificarse como un ciberataque armado según el artículo 51 de la Carta cuando alcance la ‘escala y efectos’ equivalente a un ataque armado realizado con armas cinéticas» (p. 266). Entendiendo como «escala y efectos» toda acción cibernética que provoque lesiones graves o la muerte de personas físicas o que dañe o destruya bienes materiales, como, por ejemplo, un ciberataque contra las infraestructuras críticas para el tratamiento de aguas que cause un gran número de muertos y heridos. Incluso, agrega que «consideramos más respetuosa del *ius ad bellum* aplicable al espacio una legítima defensa, frente a un ciberataque armado, que se despliegue a través de una respuesta cibernética, evitando así posibles escaladas de violencia que acaben provocando una guerra, así como la conocemos» (p. 273). La respuesta de la Unión Europea a las amenazas del ciberespacio corre a cargo de Piernas López que se analiza a través de una triple perspectiva: sobre los orígenes de la política de ciberseguridad en la Unión, la estrategia de ciberseguridad y las iniciativas en materia de ciberdiplomacia, así como la adopción de medidas restrictivas frente a los ciberataques. En este sentido, apunta que «la Unión Europea ha optado por el pragmatismo en relación con la adopción de un marco sancionatorio dirigido a personas físicas o jurídicas, entidades u organismos que lleven a cabo ciberataques con un efecto significativo» y agrega que «parece evidente que la Unión Europea va a seguir ocupándose activamente de la lucha contra las amenazas cibernéticas» (p. 306). Finalmente, Muñoz Rodríguez estu-

dia la ciberseguridad y el espacio ultraterrestre desde la triple perspectiva internacional, europea y nacional. Se trata de un tema sumamente importante en la medida que el espacio ultraterrestre se ha convertido en un ámbito de expansión de las actividades humanas, en ciertos casos cuestionables, que combinado con el ciberespacio generan una simbiosis que no debe pasar desapercibida a los juristas, dado que «la seguridad y la exploración y explotación del espacio ultraterrestre han estado interconectadas desde el comienzo de la era espacial» (p. 309). Cabe señalar que la mayor parte de las estructuras críticas sobre las que se apoyan las funciones básicas de la sociedad moderna, tales como las comunicaciones, transporte aéreo, comercio marítimo, la energía, los servicios financieros, la agricultura, los sistemas de defensa, la vigilancia meteorológica, dependen indefectiblemente de la tecnología e infraestructura espacial. En esta línea, se han desarrollado determinadas capacidades contraespaciales categorizadas como física cinética, la física no cinética, la electrónica y la ciber, que generan vulnerabilidad ante la interrupción de las nuevas capacidades contraespaciales. Por ello, en relación con el ingente desarrollo de las ciberamenazas en el espacio, la autora advierte que, «los objetivos a alcanzar con los ciberataques en el ámbito aeroespacial son muy diversos y pueden ir desde la modificación no autorizada de la información contenida en la base de datos de los clientes, la filtración de información sensible, la alteración del mercado del tráfico aéreo, el debilitamiento de la posición competitiva de un competidor industrial hasta los ataques disruptivos contra los sistemas de la aeronaves, los sistemas de control de tierra, las ayudas a la navegación o los sistemas de coordinación de tráfico aéreo nacional, lo que podría afectar la seguridad de las aeronaves, del transporte aéreo y de los viajeros» (p. 332). Ante esta amplia gama de amenazas se hace necesaria la elaboración de estrategias que incrementen y mejoren las capacidades de reacción frente a los ciberataques en el marco de las actividades aeroespaciales con

desarrollos legales nacionales, europeos e internacionales. No obstante, en el ámbito del derecho del espacio ultraterrestre perviven ciertas lagunas legislativas que aún deben colmarse, pues como con acierto se indica en el trabajo, «la asignatura pendiente del *Corpus Iuris Spatiales* respecto a la falta de claridad de conceptos como ‘arma espacial’, ‘armamento del espacio’ y ‘usos pacíficos/militares del espacio’ sigue demandando una respuesta, más perentoria si cabe, a raíz de las incógnitas que plantean las capacidades y tecnologías contraespaciales implementadas, en una eventual guerra electrónica y cibernética» (p. 338).

Como puede colegirse de los textos descritos, el armazón científico y didáctico de la obra se conforma con la especial sensibilidad de acotar cada uno de los temas ejes, Drones, Armas Autónomas y Ciberespacio, desde un ángulo conceptual con el que se introduce su estudio en el marco del clásico *ius ad bellum*, su impacto desde la perspectiva del Derecho humanitario o su análisis en el contexto jurídico de la Unión Europea, sin olvidar sus consecuencias en el Derecho internacional; y, por lo que respecta al espacio ultraterrestre, se agrega un último capítulo que implica la oportunidad de tratar un tema de gran calado y actualidad como el de la ciberseguridad en las actividades del espacio ultraterrestre.

No resulta baladí indicar que la publicación de esta monografía grupal viene a cubrir un necesario campo de estudio en el que los

ius-publicistas tenemos mucho que aportar por el control de las actividades en el marco del uso de la fuerza, en este caso, de la mano de las nuevas tecnologías que acrecientan la incertidumbre sobre los límites legales de determinados ingenios robóticos y el amplio campo de acción que se genera a través del ciberespacio.

Además, es de agradecer que estos trabajos puedan llevarse a término con el apoyo a la investigación que se brindan a proyectos como el que ha dado lugar a este trabajo, en el que la profesora Cervell Hortal, catedrática acreditada de la Universidad de Murcia, como investigadora principal ha recibido la cobertura del Programa estatal de Investigación, Desarrollo e Innovación Orientada a los restos de la sociedad del Ministerio de Economía, Industria y Competitividad.

En definitiva, los avances de la inteligencia artificial nos enfrentan ante un reto de índole ético en el que los juristas necesitaremos realizar un gran esfuerzo de conceptualización para definir los límites que no deben traspasarse por los algoritmos y que, en base a computación de datos, se aplique un *triaje* que como consecuencia del cribado o la catalogación robótica determinen cómo utilizar el uso de la fuerza sin control humano.

Juan Manuel DE FARAMIÑÁN GILBERT
Catedrático emérito de Derecho
Internacional Público
Universidad de Jaén

SALINAS ALCEGA, Sergio

Desplazamiento medioambiental y Derecho Internacional.

Consideraciones en torno a la necesidad de un marco regulatorio no exclusivo

Tirant lo Blanch, Valencia, 2020, 238 pp.

Sin lugar a dudas el cambio climático está dando lugar a una intensificación constatable del fenómeno de los procesos migratorios impactando igualmente en su carácter inequitativo. Su naturaleza global y planetaria a la vez

que permanente y no estacional, ha transformado negativamente el escenario migratorio, convirtiéndolo en mucho más masivo y, en muchas ocasiones, trágico. A pesar de ello, la actual regulación de lo que podríamos llamar