SEGURA SERRANO, Antonio, *El desafío de la ciberseguridad global: análisis desde el Derecho internacional y europeo*, Tirant lo Blanch, Valencia, 2023, 276 pp.

Esta monografía que comentamos presenta un análisis de la ciberseguridad desde el punto de vista del Derecho Internacional, estudiando los principales elementos y principios de Derecho Internacional afectados, así como su futuro desarrollo normativo, y prestando una especial atención a su tratamiento por la UE.

La monografía consta de siete capítulos. El primero de ellos recoge una introducción bastante clarificadora sobre el contenido de la obra, el segundo capítulo está dedicado a la cuestión de la atribución de la responsabilidad internacional, el tercer capítulo analiza los principios de Derecho Internacional afectados y el cuarto de estos capítulos recoge un análisis jurídico de las respuestas individuales a casos de ciberataques. Por otra parte, el capítulo quinto añade una nueva perspectiva de estudio relativa al desarrollo normativo de la materia, para finalizar el análisis con un sexto capítulo dedicado a la ciberdiplomacia europea, junto con unas conclusiones en el séptimo y último capítulo. Por lo tanto, se trata de un trabajo que realiza, como el propio autor indica, un análisis holístico de la materia en el ámbito del Derecho Internacional.

Comenzando nuestro comentario en relación con del capítulo segundo, el mismo constituye un acierto el tratar de resolver la compleja cuestión de la atribución al comienzo de la obra, debido que, concluida la posibilidad de atribución a los Estados, ésta permitirá el análisis del resto de cuestiones relativas a principios de derecho internacional y respuesta unilateral. Este segundo capítulo analiza las dos cuestiones claves en la atribución: la atribución técnica y la jurídica, siendo la primera necesaria para poder concluir respecto de la segunda. Como bien señala el autor, la atribución técnica es de enorme complejidad, y refiere las distintas propuestas de atribución planteadas, si bien concluye que a pesar de que se han ido mejorando las capacidades de atribución, no existe completa certeza sobre los resultados de dicho análisis forense. Respecto de la atribución jurídica, en primer lugar, señala la problemática de la misma haciendo referencia a informes del Grupo de Expertos Gubernamentales de Naciones Unidas y lo recogido en el propio Manual de Tallin, para pasar a analizar la responsabilidad por las actividades de órganos estatales, que estudia tomando como base los Artículos de la CDI sobre responsabilidad del Estado por la comisión de hechos ilícitos. Para ello, se centra tanto en la atribución *de iure* como *de facto*, y presta una especial atención esta última debido a la complejidad que puede plantear la identificación de los órganos *de facto,* realizando un análisis de cómo los requisitos para dicha atribución se pueden presentar en las actividades cibernéticas, para finalizar con la cuestión de los actos *ultra vires*. En lo relativo a la atribución al Estado de las actividades de los particulares, el epígrafe analiza los distintos test planteados por la jurisprudencia y concluye con el planteado por la CDI para atribuir la responsabilidad. Finalmente, una vez analizado los dos tipos de atribución el capítulo finaliza con un epígrafe en el que se aplican dichas conclusiones al ciberespacio, contraponiendo las diferentes posiciones de la doctrina relativas a la opción del test de control efectivo o el test de control global, y concluyendo sobre las distintas opciones normativas que se ha planteado para la atribución, como que la misma se haga por actores no estatales o por un mecanismo internacional centralizado.

La obra continúa con un tercer capítulo dedicado a analizar una serie princi-

 https://doi.org/10.36151/REDI.76.2.53

pios de derecho internacional en relación con los ciberataques, esto es, el principio de prohibición de uso de la fuerza, el principio de no intervención, la soberanía estatal y el principio de diligencia debida. Respecto del primero de ellos, quizás el más conflictivo, el trabajo determina qué podemos entender por un ataque virtual, advirtiendo que no se asemeja a un uso de la fuerza armada real. En todo caso, la cuestión a analizar es si un ataque de este tipo podría encuadrarse en el art. 2.4 de la Carta de Naciones Unidas, analizando en primer lugar si un ciberataque podría considerarse como un uso de la fuerza. Para ello el autor analiza los tres enfoques adoptados por la doctrina sobre la naturaleza del uso de la fuerza en el ciberespacio, así como la clasificación propuesta por Rossini para catalogar los tipos de ciberoperaciones según sus resultados. Respecto del principio de no intervención, un primer epígrafe se centra en su identificación y análisis en el ámbito del derecho internacional en general, para pasar posteriormente a analizar su contenido: la coerción y la *domaine réservé,* lo cual permitirá su encuadre en el ámbito de las ciberoperaciones. Es de especial interés y muy útil, el hecho de que en el epígrafe dedicado al ciberespacio se presenten y analicen diversos casos afectados por este principio: los incidentes de Estonia en 2007, el virus Stuxnet en 2010, y la intervención en las elecciones de EEUU en 2010. El siguiente elemento de estudio, que el autor denomina "regla de la soberanía", comienza con una referencia a la cuestión relativa a la posible aplicación de normas de derecho internacional, creadas para un espacio físico, al ámbito del ciberespacio, y centrándose posteriormente en el análisis que lleva finalmente a la denominación de la soberanía como una regla y no como un principio de derecho internacional, ya que en dicho caso no podría reclamarse responsabilidad. Una vez aclarada esta posición, la siguiente cuestión a analizar es su aplicación al ciberespacio, para lo que toma como referencia el Manual de Tallin, y los dos criterios establecidos para analizar la licitud de las operaciones: la integridad territorial y la interferencia o usurpación de funciones gubernamentales, y todo ello analizando la posición de los Estados y doctrina divididos en dos grupos, que califica como soberanistas puros o relativos. Finalmente, el apartado dedicado a la diligencia debida comienza señalando acertadamente que este principio se ha utilizado como alternativa y medio de solución de los problemas de atribución, si bien como también señala, sus contornos jurídicos no están delineados, lo que hace necesario su estudio en esta obra. Dicho análisis comienza con un rastreo histórico jurisprudencial sobre la identificación del principio, concluyendo en todo caso, que existen dos posiciones respecto al mismo, la de aquellos que lo consideran como un principio de derecho internacional, frente a los que lo consideran como un estándar de comportamiento. Los dos siguientes epígrafes están destinados al análisis de los elementos determinantes de este principio, en primer lugar, del deber de prevención del daño, que señala consiste en una obligación de conducta no de resultado, que se materializa cuando se produce el daño, pasando a un análisis crítico del daño tomando de nuevo como referencia el Manual de Tallin. El segundo elemento es el relativo al conocimiento, rechazando la necesidad de conocimiento absoluto y analizando la cuestión de si el Estado "debería haber tenido conocimiento", al que denomina "conocimiento constructivo". Para terminar este epígrafe dedicado a la diligencia debida, se introduce acertadamente un apartado sobre los beneficios y riesgos de tan referido principio en el ámbito ciber, siendo quizás más interesantes los riesgos que plantea, ya que dicho principio ha sido utilizado en la mayoría de los casos como solución, sin analizar los problemas que pueden

derivarse y que deben tenerse presentes si optáramos por su aplicación.

El capítulo cuarto de esta obra está dedicado a la respuesta unilateral por parte de los Estados víctimas de ciberoperaciones, y comienza su estudio con una de las cuestiones principales y más controvertidas, la legitima defensa en el ámbito de las ciberoperaciones, debido a la cuestión relativa a la relación entre operación cibernética y ataque armado. Para ello analiza los criterios de escala y efectos en relación con las operaciones cibernéticas, prestando especial atención a la cuestión del daño físico y la necesidad de víctimas. El siguiente epígrafe lo dedica a otra cuestión controvertida, no solo en el ámbito de las ciberoperaciones, sino en el ámbito general de la legitima defensa, como es el ejercicio de la misma frente a actores no estatales, para pasar posteriormente al análisis de los dos elementos a tener en cuenta a la hora del ejercicio de la legítima defensa, como la necesidad y proporcionalidad, que presenta sus particularidades y una especial complejidad en el ámbito de la ciberoperaciones, como analiza y clarifica el autor. Finalmente, el autor vuelve sobre un tema conflictivo como es el de la legitima defensa preventiva, cuyo análisis y aplicación a las ciberoperaciones justifica por las características de este tipo de operaciones: los ataques son instantáneos y no dejan tiempo al Estado para reaccionar y repeler el ataque.

El siguiente epígrafe de este capítulo cuarto está dedicado al estudio de las contramedidas, quizás el ámbito del derecho internacional en el que más cómodamente se puedan mover las respuestas a las ciberoperaciones. Después de un análisis sobre el concepto de las contramedidas y sus requisitos, enfocados desde el punto de vista del ciberespacio, esta obra analiza las condiciones procesales de aplicación de las contramedidas en el ciberespacio, señalando las dificultades de las mismas hasta el punto de haber sido eliminada por el Manual de Tallin la necesidad de notificación previa, convirtiendo las medidas, como señala el autor, en un elemento punitivo. Muy interesante resulta el epígrafe dedicado a los límites de las contramedidas, ya que, debido a las características de las ciberoperaciones, se pone de manifiesto la afectación a derechos como por ejemplo el derecho a la privacidad. El último epígrafe dedicado a las contramedidas analiza el porqué de la afirmación que hemos realizado anteriormente referida que, las contramedidas son el recurso que mejor sirve para dar respuesta, no sin problemas, a las ciberoperaciones maliciosas. Esta afirmación deriva de la dificultad que presenta la aplicación de la legitima defensa, pero debiendo tener presentes de nuevo, tal y como señala el autor, la necesidad de no convertirlas en un elemento punitivo.

Finalmente, el capítulo cuarto dedicado a las medidas unilaterales se centra en el estudio del estado de necesidad, cuya aplicación tiene sentido en el ámbito de las ciberoperaciones debido a dificultad que presentan las dos alternativas previamente estudiadas: la legitima defensa y las contramedidas. De este modo, el estado de necesidad no requiere de la comisión de un hecho ilícito y su atribución el Estado, sino que, como señala el autor, permite al Estado enfocarse únicamente en hacer frente a una amenaza. Para ello, el autor pasa a analizar los requisitos para la aplicación del estado de necesidad en relación con las ciberoperaciones, utilizando los Artículos de la CDI, la jurisprudencia de la CIJ y el Manual de Tallin. En todo caso, a pesar de que el estado de necesidad pueda parecer la mejor respuesta, en la práctica, tal y como pone de manifiesto el autor al analizar las limitaciones de aplicación, resulta difícil la aplicación del estado de necesidad debido a la obligación de demostrar que la acción del Estado es el "único modo" de hacer frente a la amenaza. Esta di-

ficultad se traslada también al ámbito del ciberespacio, debido al poco tiempo que se tiene para deliberar y por lo tanto determinar si se trata del "único modo" de respuesta. Junto con esta cuestión, el segundo elemento que el autor señala y analiza a fin de poner de manifiesto las limitaciones de este recurso es que no afecte a los intereses esenciales de otro Estado, utilizando ejemplos que ayudan a identificar sus particularidades en el ámbito ciber. Para terminar, se hace una breve referencia al estado de necesidad y de nuevo al uso de la fuerza, como en el caso de la legitima defensa, concluyendo que la doctrina y la práctica, si bien señala escasa, indican que el estado de necesidad no ampara el uso de la fuerza.

Como señalábamos al comienzo, el capítulo 5 supone añadir al trabajo en nuevo elemento de análisis como es el desarrollo normativo de esta materia, liderado en este caso por Naciones Unidas. Para ello, se estudia la evolución de los grupos de expertos gubernamentales, señalando los avances conseguidos y cómo las diferentes posiciones de las grandes potencias resultaron, en 2018, en la división en dos grupos liderados por Estados Unidos y Rusia respectivamente. Con el fin de clarificar dichas posiciones, en los siguientes epígrafes se analizan los resultados del Grupo de Expertos Gubernamentales y el del Grupo de Trabajo de Composición abierta liderado por Rusia y China, que culmina con un informe en 2021, objeto de análisis en este epígrafe, y que fue endosado por la Asamblea General de Naciones Unidas. Finalmente, este culmina con un estudio del cibercrimen, lo cual parece alejarse un poco del ámbito de estudio de la obra, quizás por acercarse a cuestiones relativas cooperación judicial, si bien en aplicación de un tratado internacional, el Convenio de Budapest. En todo caso, el autor critica la escasa implementación por los Estados de dicho convenio y los intentos del Consejo de Europa de hacerlo más efectivo, con la adopción de un nuevo protocolo que no está exento de críticas debido a su posible afectación a los derechos humanos. Si bien se ha considerado el Convenio de Budapest como la norma principal en la lucha contra la ciberdelincuencia, el autor nos presenta en el segundo apartado un interesante estudio sobre la propuesta de creación de un Convenio sobre ciberdelincuencia en el marco de Naciones Unidas, cuya propuesta fue aprobada por la Asamblea General en 2019, pero de nuevo con posiciones encontradas entre Estados Unidos, que prefiere centrar esta lucha en el marco del Convenio de Budapest, y Rusia que apuesta por un nuevo convenio.

La obra cierra finalmente, previa a las conclusiones, con un capítulo dedicado a la Unión Europea, donde se analizan tres aspectos de especial interés para la misma: la ciberdelincuencia, la ciberdiplomacia como un instrumento de ciberseguridad y la ciberdefensa. En relación con el estudio de la ciberseguridad, el autor realiza una exposición de cómo ha evolucionado la normativa y el enfoque de la UE para hacer frente a este reto, y no solo frente ataques de civiles relacionados con cibercrimen, sino frente a su uso por terceros Estados. Pero el principal estudio normativo se lleva a cabo en el epígrafe dedicado a la política de ciberseguridad de la UE, un epígrafe muy completo que toma como punto de partida la Estrategia de Ciberseguridad de 2013, cuyo contenido el autor divide en tres pilares, la seguridad de las redes y de la información, el cibercrimen y la ciberdefensa, para pasar a analizar cada uno de ellos. En todo caso, como decíamos se trata de un epígrafe muy completo, y además de analizar la Estrategia de 2013, lleva a cabo un estudio sobre normativa posterior, partiendo de la Comunicación de la Comisión y la Alta Representante de 2017, que se ha calificado como "segunda estrategia de ciberseguridad", para finali-

zar con el estudio de la última Estrategia de Ciberseguridad adoptada en 2020.

En lo relativo a la ciberdiplomacia, comienza con una definición que permite identificar este nuevo concepto, y que se centra en la búsqueda de métodos tanto para asegurar los intereses del Estado en el ciberespacio, como en la búsqueda de normas que regulen el comportamiento de los Estados en el ciberespacio. En el caso de la UE, como señala al autor, el punto de partida fueron las Conclusiones del Consejo sobre ciberdiplomacia de 2015, siendo quizás las Directrices de la aplicación del Marco para una respuesta diplomática conjunta de la UE a las actividades cibernéticas maliciosas, las que suponen un mayor desarrollo y que el autor analiza con mayor profundidad. Finalmente, el estudio de la ciberdiplomacia termina con un interesante análisis del régimen de sanciones de la UE en materia de ciberataques, enfocado no solo en el estudio de las medidas llevadas a cabo por la UE, sino también en la evaluación jurídica de las mismas y su efectividad.

Este capítulo termina con una referencia a la ciberdefensa en la UE, en la que se recoge el desarrollo normativo que ha permitido desplegar una política de ciberdefensa en el ámbito de la Unión que culminan con la actualización en 2018 del Marco político de ciberdefensa, y con la Comunicación Conjunta de Política de ciberdefensa de 2022. Para concluir, analiza los instrumentos de respuesta de la UE tomando como base la cláusula de solidaridad del artículo 222 TFUE y la cláusula de asistencia mutua defensiva del artículo 42.7 TFUE, señalando en todo caso las limitaciones de ambos y concluyendo que probablemente sea la cláusula de solidaridad la que tenga mejor encaje para poder ejercer una respuesta.

En definitiva, este trabajo constituye una obra que permite acercarse al conocimiento de la regulación del ciberespacio por el derecho internacional, analizando todos los elementos afectados por esta nueva práctica, y poniendo en todo caso de relieve las enormes dificultades que plantea su regulación, los vacíos legales existentes, los riesgos y amenazas, así como la imposibilidad de dar una respuesta efectiva y ampliamente aceptada. En todo caso, una obra necesaria y útil para aquellos que se adentran en el estudio del ciberespacio.

Gloria Fernández Arribas
Universidad Pablo de Olavide

Zernikow, Marcel, *Les règles de conflit de lois confrontées au marché intérieur. Étude en droit international privé européen du travail*, L'Harmattan, París, 2024, 654 pp.

La movilidad laboral internacional se ha convertido en un aspecto natural altamente necesario en el tráfico jurídico externo. Entre las claves de la movilidad laboral, destacan aspectos tales como las innovadoras tecnologías de comunicación, el desarrollo de Internet, la mejora en los transportes junto con la industrialización y la transformación digital, entre otros. En este contexto, el impulso transfronterizo ha despertado el interés de la legislación laboral internacional como conjunto de normas provenientes de instancias supranacionales que contribuyen a la institucionalización de las relaciones de trabajo. Así las cosas, en la parte introductoria de la monografía objeto de esta recensión, se hallan interesantes aclaraciones preliminares, entre las que merecen poner de relieve, la acer-