Published on *Fondation Euro-Arabe des Hautes Etudes* (https://www.fundea.org)

blogCiberseguridad y Derecho Internacional

04 sep 2020

Ciberseguridad y Derecho Internacional [1]

"Los ciberataques son un problema creciente y persistente" manifiesta el profesor Antonio Segura Serrano en el artículo "Ciberseguridad y normación en Derecho Internacional" que os presentamos a continuación. Con este artículo traemos a nuestro blog un tema de notable actualidad, la Ciberseguridad. Sin duda este es un tema que preocupa a la comunidad internacional y también a la gente de a pie que lo encuentra cada vez más a menudo, bien en noticias o artículos de cualquier medio de comunicación o como base argumental de películas y series de televisión, en muchas ocasiones vinculado a la que llaman "Guerra de Cuarta Generación", una guerra asimétrica e invisible derivada de las nuevas tecnologías e interacciones globalizadas.

Ciberseguridad y normación en Derecho internacional

Antonio Segura Serrano *

Los ciberataques son un problema creciente y persistente. Por ejemplo, el virus ransomware conocido con el nombre *WannaCry [2]*, que puso en jaque a medio mundo en 2017, seguía siendo uno de los más agresivos virus a finales de 2019. Los ciberataques pueden tener un origen público o privado. En el primer caso, entran en el ámbito del uso de la fuerza, regulado por el Derecho internacional en el marco de la Carta de la ONU, cuyo capítulo séptimo se destina a la seguridad colectiva. En el caso de los ciberataques de origen privado hay que recurrir a diversos mecanismos de cooperación jurídica internacional, alguno de los cuales será mencionado a continuación.

Cuando se trata de la aplicación del Derecho internacional en el ámbito del ciberespacio, con el objeto de hacer frente a esos ciberataques, caben dos opciones. Se puede recurrir a las normas existentes en Derecho internacional, a través de la oportuna adaptación. O se puede proceder a la elaboración de tratados de nuevo cuño. La primera opción ha sido la sostenida por EEUU y sus aliados occidentales. Las estrategias de ciberseguridad de estos países son muy explícitas al respecto, como hace la **estrategia española de 2013 y la posterior de 2019** **[3].** Por su parte, la Asamblea General de Naciones Unidas (AGNU), en el marco de la Primera Comisión, ha logrado llegar a un consenso mínimo en este mismo sentido a través del "Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional" (GEG).

En el Informe de 2013 del GEG se llegó a un acuerdo en torno a la aplicabilidad al ciberespacio del Derecho internacional existente, en concreto, la Carta de la ONU, los derechos humanos, así como las reglas básicas sobre responsabilidad internacional. Del mismo modo, el Informe de 2015 del GEG vino a insistir sobre la aplicabilidad en el ciberespacio de algunos principios del Derecho internacional humanitario (como la proporcionalidad o la distinción), así como la obligación de diligencia debida. Algunas iniciativas privadas importantes han secundado esta opción, como ha hecho el Manual de Tallin (2013 y 2017), promovido por la OTAN, y que hace un análisis exhaustivo de esta aplicación analógica. La segunda opción, consistente en la elaboración de nuevos tratados internacionales, ha sido abanderada por Rusia, China y otros países, que han hecho propuestas como el Código de Conducta para la Seguridad de la Información de 2011. La contraposición entre estas dos opciones se ha puesto de manifiesto en el **Informe del GEG de 2017** **[4],** que ha sido considerado como un fracaso. En efecto, cuestiones tales como el recurso a la legítima defensa, las contramedidas, o el reconocimiento explícito de ciertas normas del derecho internacional humanitario han sido rechazadas por países como Rusia, China o Cuba, sobre la base de que los países occidentales persiguen una militarización del ciberespacio.

Este fracaso puede llevar a pensar que la vía multilateral se encuentra cerrada y que los Estados van a recurrir a la vía unilateral o regional. Sin embargo, a finales de 2018 se han creado **dos grupos de trabajo** **[5]** en el marco de la AGNU. Por una parte, se ha puesto en marcha un nuevo GEG patrocinado por EEUU (con 25 representantes gubernamentales) y, por otra parte, se ha creado un Grupo Abierto de Trabajo promovido por Rusia, no incompatible con el anterior y pretendidamente más inclusivo (puede incorporar a todos los miembros de la ONU). Este resultado demuestra una nueva actitud más pro-normativa entre los Estados miembros de la ONU, aunque puede ser a costa de una mayor lentitud y complejidad en el proceso. Esta actividad pro-normativa puede ser también una especie de reacción gubernamental ante las diversas iniciativas privadas que se está produciendo recientemente. En efecto, además del denominado proceso de La Haya, en el que se inserta el Manual de Tallin II, de 2017, ocupa un lugar destacado la **Convención Digital de Ginebra** **[6]**, promovida por Microsoft desde el año 2017.

Si esto es lo que ocurre en el plano de la normación general con relación al ciberespacio, en el ámbito más limitado de la ciberdelincuencia se ha producido una evolución singular, también animada por la prevalencia de los ciberataques de origen privado, que provocan un coste creciente, valorado en 600 mil millones de dólares anuales, según un **informe de 2018** **[7].** En efecto, en el terreno del cibercrimen se adoptó ya en 2001 la **Convención de Budapest** **[8]** en el marco del Consejo de Europa. Se trata de una convención que ejemplifica de forma temprana una exitosa cooperación internacional. Esta convención lleva a cabo una armonización mínima en materia jurisdiccional y, de forma específica, en materia de acceso a la prueba digital. No obstante, como en otros supuestos de cooperación jurídica internacional, esta convención se ve lastrada por una importante lentitud en la asistencia entre los Estados parte (las solicitudes tardan meses en ser atendidas) lo que

lleva a muchos Estados parte a recurrir alternativamente a instrumentos bilaterales (los conocidos como MLAs). También se ha criticado que esta Convención permite a los Estados eludir las salvaguardas nacionales en favor de los derechos humanos.

Como consecuencia de la escasa efectividad de la cooperación jurídica internacional puesta en marcha con la Convención de Budapest, los Estados han empezado a recurrir a mecanismos de corte unilateral para hacer frente al fenómeno del cibercrimen de carácter transnacional. Una de esas vías unilaterales consiste en el hackeo transfronterizo. No existen hasta ahora ejemplos de denuncia de este tipo de prácticas por parte de Estado alguno. No obstante, la certeza sobre la existencia de este tipo de capacidades permite adivinar que su uso se ha llevado ya a cabo en situaciones particulares. Por otra parte, existe otra vía unilateral para el acceso a la prueba digital, como es la que consiste en la obtención de la colaboración directa por parte de los proveedores de servicio del Estado de destino. La ventaja que ofrece esta posibilidad es que convierte en innecesaria la intervención o la autorización de las autoridades del Estado de destino para que el Estado solicitante tenga acceso a la evidencia electrónica. Esta posibilidad es la que ha contemplado la US Cloud Act [9] de 2018 y también es la que prevé la propuesta de **Directiva E-evidence** **[10],** que incluye una Orden de Producción Europea.

Precisamente, desde el Consejo de Europa se ha querido hacer frente a la actual infrautilización de la Convención de Budapest, por lo que se ha iniciado el proceso de adopción de un nuevo Protocolo a la Convención de 2001. Este nuevo protocolo pretende introducir simplificación en el proceso de asistencia jurídica entre los Estados parte, mejorando así las cifras que se han obtenido hasta la fecha en este sentido. El resultado final al que se pretende llegar con el protocolo permitiría al Estado de origen hacer prevalecer sus normas aplicables sobre la materia como consecuencia del ejercicio de su jurisdicción para perseguir el ciberdelito de que se trate. Sin embargo, las ONGs como Edri o EFF han criticado este intento por elaborar un nuevo Protocolo, ya que consideran que supondrá con toda seguridad una erosión de los estándares aplicables en el Estado de destino. Teniendo en cuenta que entre los Estados del Consejo de Europa no sólo no hay armonización de normas penales, sino que los sistemas jurídicos nacionales son muy diversos, los ámbitos que se podrían ver más afectados serían los relativos a los derechos humanos protegidos en el Estado de destino, entre los que hay que destacar el derecho a la privacidad y la protección de datos personales, así como las salvaguardas de carácter procesal aplicables en dicho Estado de destino.

En el plano de la ONU, una propuesta de Rusia sobre una Convención contra el Cibercrimen fue rechazada ya en el 2010. En el 2011, la Comisión para la Prevención del Delito y la Justicia Penal (CPDJP) creó un Grupo de Expertos, a petición de la Asamblea General, para realizar un estudio exhaustivo sobre el cibercrimen, con el objeto de preparar respuestas jurídicas o no, nacionales o internacionales, para afrontar este fenómeno. Este estudio exhaustivo sobre el cibercrimen [11] fue encargado a la Oficina de la ONU contra las Drogas y el Crimen y completado en 2013. La labor del Grupo de Expertos continuará hasta 2021 en que está previsto que finalice su tarea. Sin embargo, existe un desacuerdo en el marco de la ONU sobre cómo afrontar la lacra del cibercrimen. Por una parte, EEUU y sus aliados entienden que la Convención de Budapest es un texto suficiente para luchar contra el cibercrimen. Además, la labor del Grupo de Expertos está por finalizar, de modo que en la actualidad lo más conveniente es esperar a evaluar los resultados de ese trabajo. Por otro lado, Rusia y otros Estados han manifestado que prefieren la elaboración de un nuevo texto universal que materialice un consenso global, por tanto, un consenso que no se limite a los Estados parte del Consejo de Europa. Además, en su opinión, ciertos mecanismos del Convenio de Budapest, como el artículo 32.b, suponen un atentado a la soberanía del Estado territorial, ya que implica la posibilidad de eludir la previa autorización de dicho Estado con ocasión de la obtención de la evidencia electrónica.

En este contexto, ha sorprendido a ciertos países occidentales que se haya aprobado recientemente por la AGNU una Propuesta de Convención sobre el Cibercrimen a finales de 2019. En efecto, la mayoría alcanzada para adoptar esta Resolución ha puesto de manifiesto un voto divisivo (79-60-30), pero esta vez a favor de la iniciativa normativa. La propuesta de convención está basada en un borrador presentado por Rusia en 2017. Este borrador incluía una lista de los ciber delitos perseguibles (entre los que se encuentra el hackeo), las distintas opciones de cooperación jurídica entre Estados, así como el establecimiento de un Centro de contacto para investigaciones. Con el objeto de hacer avanzar la propuesta aprobada por la ONU en 2019, se ha incorporado la creación de un Comité Abierto de Expertos *ad hoc*. No obstante, esta propuesta de la ONU ha sido criticada por las ONGs. Se aduce por parte de éstas que, teniendo en cuenta que su promotor es Rusia, la propuesta no puede conducir sino a una mayor criminalización de las conductas en Internet, en línea con el mayor control estatal que Estados como Rusia o China promueven en la Red. En su opinión, con esta propuesta se quiere ir más allá de las previsiones recogidas en el Convenio de Budapest, de modo que la posibilidad de rechazo de solicitudes de asistencia por parte del Estado de destino se reduce. Además, habría que dejar que el Grupo de Expertos del CPDJP terminase su trabajo en 2021.

La propuesta de un nuevo Convenio de la ONU sobre Cibercrimen es un ejemplo de la nueva actitud más pro-normativa que parece ir consolidándose en la actualidad. En efecto, por un lado, la Convención de Budapest acumula una experiencia de dos décadas, con gran aceptación entre los Estados (hay 65 Estados parte y muchos la han incorporado a su legislación nacional). En particular, ha sido objeto de una Declaración de Apoyo por parte de la UE que, junto a EEUU, rechaza la propuesta de la ONU. Por otro lado, Rusia, China y muchos PVDs aducen que la Convención de Budapest representa a un club limitado de Estados, lejos del consenso global que se puede alcanzar en la ONU. De hecho, esta opción por una nueva convención ha ido ganando peso entre los Estados miembros de esta organización, bien porque los equilibrios de política exterior han ido mudando (hay Estados parte de la Convención de Budapest, incluso del Consejo de Europa, que han votado a favor de la propuesta), bien porque existe un creciente atractivo en torno a un nuevo Tratado Global sobre esta materia y el consiguiente refuerzo de la soberanía estatal que puede conllevar.

Desde el punto de vista jurídico, no deben obviarse las consecuencias derivadas de la adopción de una nueva Convención sobre el Cibercrimen que, como la Convención de Budapest, aspira a la generalidad. Si existen dos convenciones sobre la misma materia habrá que recurrir al artículo 30 de la Convención de Viena sobre Derecho de Tratados. Con independencia de la solución que haya de adoptarse en cada caso, recurriendo a una suerte de bilateralización, lo cierto es que la existencia de dos marcos jurídicos de carácter general sobre la misma materia no va a ayudar a la simplificación de la asistencia jurídica entre Estados.

En conclusión, existe una ausencia de consenso normativo que enfrenta a EEUU y los países occidentales, por una parte, y Rusia, China y muchos PVDs, por otra parte. Los primeros abogan por una aplicación analógica de las normas existentes al ciberespacio, mientras que los segundos prefieren la elaboración de normas nuevas. Las causas de esta ausencia de consenso son tanto políticas (Internet abierto y protección de los derechos humanos frente a Internet cerrado y mayor control estatal) como estratégicas (defensa de la actual ventaja tecnológica frente a ruptura del *status quo*). Esta ausencia de consenso resulta peligrosa para la estabilidad de las relaciones internacionales, así como para la capacidad de frenar los ciberataques, amén de la dejación de funciones que implica y que explica la proliferación de iniciativas normativas privadas. Además, en el ámbito más concreto del cibercrimen, se produce una cierta paradoja. Las percepciones sobre la defensa a ultranza de la soberanía estatal, por unas razones o por otras, impiden avanzar en cuanto a la normación se refiere. Sin embargo, una mayor cooperación en este terreno conduciría a una protección más efectiva de los intereses estatales, ya que en la situación

actual las veleidades unilaterales siguen siendo frecuentes.

** **Antonio Segura Serrado** es profesor Titular de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Granada; Vicesecretario de la Fundación Euroárabe de Altos Estudios; miembro Garante de la Unidad Investigadora de Excelencia "Sociedad Digital: Seguridad y Protección de Derechos" de la Facultad de Derecho de la UGR; Experto de la Comisión de Comercio Internacional del Parlamento Europeo (INTA); y Evaluador de la Agencia Nacional de Evaluación y Prospectiva.*

Partagez-le

Liens
[1] https://www.fundea.org/fr/node/2544
[2] https://nakedsecurity.sophos.com/2019/09/18/wannacry-the-worm-that-just-wont-die/
[3] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
[4] https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance
[5] https://www.un.org/disarmament/ict-security/
[6] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.001sx7y4z169ueiaqw12pjsaxftjy
[7] https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html
[8] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[9] https://epic.org/privacy/cloud-act/
[10] https://www.consilium.europa.eu/es/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/
[11] https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf