Internacionalización de los derechos humanos

AREANDINA
Fundación Universitaria del Área Andina

Sánchez, Luis Eduardo / autor

Internacionalización de los derechos humanos -- / autor Luis Eduardo Sánchez [y otros 5 autores] -- Bogotá: Fundación Universitaria del Área Andina, 2020.

ISBN (digital): 978-958-5139-19-0
61 páginas: gráficos, tablas; 28 cm.
Incluye índice

1. Derechos humanos y globalización. – 2. Defensores de derechos humanos. – 3. Derecho internacional y derechos humanos.

Catalogación en la fuente Biblioteca Fundación Universitaria del Área Andina (Bogotá)

341 – scdd22

Internacionalización de los derechos humanos

Fundación Universitaria del Área Andina
Calle 70 No. 12-55, Bogotá, Colombia
Tel: +57 (1) 7424218 Ext. 1231
Correo electrónico:
publicaciones@areandina.edu.co

Dirección editorial:
Omar Eduardo Peña Reina

Coordinación editorial:
Camilo Andrés Cuéllar Mejía

Diseño de carátula:
Xpress Estudio Gráfico y Digital

Corrección de estilo, concepto gráfico, diseño, composición e impresión:
Xpress Estudio Gráfico y Digital

ISBN (digital): 978-958-5139-19-0

Bandera institucional

Miembros Fundadores	Pablo Oliveros Marmolejo ǂ Gustavo Eastman Vélez
Presidente del Consejo Superior y Asamblea General	Diego Molano Vega
Rector Nacional **Representante Legal**	José Leonardo Valencia Molano
Vicerrectora Nacional Académica	Martha Patricia Castellanos Saavedra
Vicerrectora Nacional de Experiencia Areandina	Ana Karina Marín Quirós
Vicerrectora Nacional de Crecimiento y Desarrollo	Karol Milena Pérez Calderón
Vicerrectora Nacional Administrativa y Financiera	Erika Milena Ramírez Sánchez
Rector - Seccional Pereira	Felipe Baena Botero
Rectora - Sede Valledupar	Gelca Patricia Gutiérrez Barranco
Secretaria General	María Angélica Pacheco Chica
Director Nacional de Investigaciones	Omar Eduardo Peña Reina
Decano Facultad de Derecho	Luis Alfonso Lizcano Higuera
Subdirector Nacional de Publicaciones	Camilo Andrés Cuéllar Mejía

Contenido

Prólogo

Toda reflexión sobre los derechos de las personas en diferentes contextos y países debe ser motivo de celebración. Simplemente porque el análisis libre y sincero, con pretensión de objetividad, tiene por propósito reflexionar sobre situaciones actuales con la pretensión de enderezarlas hacia el lado del Derecho y de tener éxito, se inclinará la balanza hacia el lado de la justicia. Los derechos humanos son tan mencionados como lesionados diariamente, esto es así porque toda violación es ínsita a todo derecho.

Estas memorias que desde la Fundación Universitaria del Área Andina y su Editorial me han honrado en prologar, tienen esa pretensión. La de reflexionar desde distintos enfoques y matices, sobre la vigencia efectiva de los derechos humanos en Colombia y por lo expuesto en el párrafo anterior, la iniciativa debe ser celebrada.

En el título 1, Luis Eduardo Sánchez Rodríguez analiza los 'Derechos Humanos y la Gerencia de la Salud'. El autor refiere la sistemática violación del derecho a la salud de la población y avala sus dichos con estadísticas que demuestran que la pretensión del ejercicio de este derecho asciende a un tercio de la totalidad de las Acciones de Tutela iniciadas en Colombia durante el pasado año de 2017.

En el título 2, Carmen Luisa Betancur Pulgarín presenta un trabajo sobre 'Derechos Humanos y Salud Laboral'. En el mismo aborda el acceso de los trabajadores a la salud en el contexto del ejercicio de las respectivas actividades profesionales. Este análisis la lleva a tratar las situaciones de las enfermedades y accidentes de trabajo, a partir de lo cual establece una muy interesante relación entre las enfermedades -sean profesionales o no-, la discapacidad y la muerte de los trabajadores.

En el título 3, Nini Jhohanna Becerra González reflexiona de manera ágil y profunda sobre los 'Derechos Humanos y Educación'. Tras afirmar la relación simbiótica entre derechos humanos y educación, establece que esta última valida, enseña y sostiene la idea fundamental de los derechos humanos. Luego analiza la forma en que se aborda comúnmente la enseñanza

en derechos humanos y plantea desafíos actuales como la humanización, la transversalidad y la proyección social. Finalmente, contrapone dos modelos de enseñanza: la educación para el conflicto y la educación para la paz, y destaca a esta como la única posibilidad de entender a la relación entre derechos humanos y educación.

En el título 4, Alexander Antonio Rodríguez Valencia analiza las situaciones de los 'Derechos Humanos y Discapacidad' en el contexto de las fuerzas policiales en Colombia. Comienza con un recordatorio de los grupos vulnerables que existen en la sociedad, respecto de los cuales se ha acuñado el término de discriminación positiva como obligación del Estado y de la sociedad toda. De entre ellos, repara especialmente en los derechos de las personas con discapacidad y refiere especialmente la situación de aquellas que revisten en la policía nacional colombiana, donde analiza lo que les sucede a aquellos efectivos policiales que poseen algún grado de discapacidad adquirida con motivo de su función y la falta de reubicación laboral que padecen. Nuevamente estamos frente a un reclamo directo de efectiva vigencia de derechos largamente reconocidos, tanto internacionalmente como en la esfera doméstica.

Finalmente, ya en el título 5, Diego Carmona Carmona realiza un estudio sobre 'La Auditoría Médica y los Derechos Humanos'. Comienza su artículo con una afirmación básica: la necesidad de conocer los derechos a fin de respetarlos. Vemos cómo la problemática de la vigencia efectiva sigue presente en todas las aristas mencionadas. Relaciona especialmente a la bioética y las nuevas tecnologías que tienen mucho por aportar en el campo del derecho y los derechos humanos. Los avances tecnológicos plantean nuevos interrogantes que, tal vez, puedan ser contestados con iguales herramientas que las utilizadas en viejos dilemas morales. Los grandes planteos éticos de la persona o morales de la sociedad siguen firmes, aunque con matices actuales.

El que se ve atacado en un derecho debe resistir. Decía Ihering que esta resistencia constituye un deber en primer lugar, para consigo mismo. Luego también, es un deber para con la sociedad. Sin embargo, si queremos afirmarnos como persona, nuestro deber primario es denunciar toda lesión de derechos, luego resistirlas y finalmente retornar a las situaciones de normalidad en las cuales el derecho es gozado sin inconvenientes. Este es el propósito de la civilización. Respetar y hacer respetar los derechos humanos es nuestro deber en todo ámbito y en toda profesión que desempeñemos.

Cada uno de los autores nombrados han cumplido con este deber, pues denuncian situaciones de lesiones de derechos humanos en su contexto y proponen vías alternativas de remedio. De esta manera, cumplen con el deber primero para consigo mismos, en lo cual intentan enderezar sus ámbitos de trabajo hacia el lado de la Justicia y, además, contribuyen a ese deber para con su familia, sus amigos, sus vecinos. En suma, para con la sociedad colombiana que habitan y su cultura que los define como personas. Este es una de las finalidades de las instituciones educativas y su razón de ser también.

La Fundación Universitaria del Área Andina en Colombia cumple su parte al generar espacios de reflexión, debate y propuestas. Este es un sencillo y efectivo ejemplo. Celebremos esto.

Favio Farinella
Mar del Plata, Argentina
Noviembre de 2018

Derechos humanos y la gerencia de la salud

Luis Eduardo Sánchez Rodríguez[1]

Fundación Universitaria del Área Andina - Colombia

[1] Médico – Magister en Administración en Salud de la Universidad del Valle. Docente del Centro de Posgrados de la Fundación Universitaria del Área Andina, Seccional Pereira.
Correo electrónico:
lsanchez2@areandina.edu.co

Resumen

En el contexto de los derechos humanos, la salud se ha catalogado como el derecho fundamental más vulnerado. Genera un 32 % del total de las tutelas presentadas en el 2017 y tiene, en general, una percepción negativa de los usuarios. Aunque existen mecanismos legales de apoyo y se observa un efecto positivo en su aplicación para el beneficio del individuo que los busca, el colectivo sigue siendo vulnerable y el sistema luce impotente e incapaz de garantizar el derecho a los ciudadanos colombianos.

Palabras clave

Derechos humanos, gerencia en salud, vulneración del derecho a la salud

Introducción

La salud en Colombia es considerada un derecho fundamental, tal como establece la Ley 1751 de 2015 conocida como Ley Estatutaria de la Salud, catalogándolo además en su artículo segundo como un "derecho autónomo e irrenunciable en lo individual y en lo colectivo". Aunque la ley es precisa, el derecho a la salud es quizás el derecho más vulnerado en Colombia lo que ha motivado un sin número de acciones legales, que van desde las peticiones a las Entidades Administradoras de Planes de Beneficio, pasando por quejas ante la Superintendencia Nacional de Salud hasta, en última instancia la interposición de Acciones de tutela. En cifras claras, de las 607, 500 interpuestas en el año 2017, 197, 655 corresponden a solicitudes de tutelar el derecho a la salud, lo que representa el 32 % del total (Unidad de Tutelas de la Corte Constitucional, 2018). La prestación de servicios de Salud no está garantizada. Son múltiples las causas que generan el irrespeto de esos derechos: problemas financieros asociados a lentitud en los flujos de dinero del sistema, los engorrosos trámites en las autorizaciones de procedimientos y tratamientos, hasta actos de corrupción que desvían los recursos.

Descripción de los temas, enfoque o perspectiva teórica del autor

La Organización Mundial de la Salud ha propuesto una serie de acciones que buscan garantizar el derecho a la salud: 1. La no discriminación, 2. La disponibilidad u oferta de servicios suficiente, 3. La Accesibilidad (geográfica), 4. La Aceptabilidad (instituciones éticas y que tengan en cuenta la cultura de los usuarios), 5.La calidad (factores técnicos y de idoneidad), 6. La rendición de cuentas (manejo transparente de los recursos) y 7.La universalidad (posibilidad de ejercer los derechos humanos en cualquier sitio y momento) (Organización Mundial de la Salud, 2017).

En Colombia, la totalidad de estos puntos clave son vulnerados en mayor o menor grado, como ejemplo en un artículo de la Asociación de Clínicas y Hospitales de Colombia acerca del tema, el 31 % de los usuarios del Régimen Contributivo y el 27 % en el Régimen Subsidiado calificó el acceso a los servicios de salud como 'difícil', y

la demora en la prestación de servicios medida, a través del tiempo de espera en la prestación del servicio de medicina general fue calificada como 'Larga' en el 51 % de los entrevistados del Régimen Contributivo y el 47 % en los pertenecientes al Régimen Subsidiado (Asociación de Clínicas y Hospitales de Colombia, ACHC, 2018). En general, la percepción del respeto al derecho a la salud podría calificarse como negativa.

Hallazgos, contribución al área de conocimiento

La presencia de entes de control que apoyan al usuario del sistema de salud, como La Defensoría del Pueblo, La Procuraduría, La Contraloría, La Superintendencia Nacional de Salud y La Fiscalía, hacen que en los casos individuales se obtenga finalmente una respuesta, lo cual no es así en lo colectivo. El respeto al derecho de la salud bajo presión habla a ciencia cierta de que el sistema todavía es insuficiente para responder con sus compromisos y obliga a replantear su estructura y funcionamiento.

Conclusiones y limitaciones del capítulo

Se evidencia que el derecho a la salud es de los más vulnerados en Colombia y que a pesar de las múltiples herramientas legales, e incluso coercitivas, existentes la respuesta del sector no logra satisfacer el respeto a este derecho.

Referencias

Asociación de Clínicas y Hospitales de Colombia, ACHC. (2018). Revolución del Sistema de Salud, propuesta de ACHC. *Hospitalaria No.117*, 4-24.

Organización Mundial de la Salud. (29 de 12 de 2017). *Salud y derechos humanos.* Obtenido de Organización Mundial de la Salud. Recuperado de http://www.who.int/es/news-room/fact-sheets/detail/human-rights-and-health

Unidad de Tutelas de la Corte Constitucional. (25 de Septiembre de 2018). *Corte Constitucional de la República de Colombia.* Recuperado de: http://www.corteconstitucional.gov.co

Derechos humanos y salud laboral[1]

Carmen Luisa Betancur Pulgarín[2]

Fundación Universitaria del Área Andina - Colombia

[2]Especialista en docencia universitaria, Especialista en Epidemiología, Magíster en Enfermería. Investigadora Junior, Colciencias. Líder grupo de investigación ZIPATEFI. Docente Centro de Posgrados, Fundación Universitaria del Área Andina.
Correo electrónico:
cbetancur@areandina.edu.co

Resumen

La Organización Mundial de la Salud (OMS), la Organización Internacional de trabajo (OIT) y autores como Reynoso, Colmenares, Mundlak y Azuela coinciden en destacar la importancia de la salud laboral, entendiéndola como un derecho fundamental de las personas, es decir, uno de los derechos humanos de mayor relevancia en la actualidad, dado que la población trabajadora supera más de la mitad de la población del planeta. El respeto por estos derechos y el compromiso de gobiernos y empresarios puede constituirse en una herramienta robusta para dar equilibrio a una mejor calidad de vida de trabajadores, familias y sociedad.

Palabras clave

Derechos humanos, salud laboral, población trabajadora.

1 Derechos Humanos y Salud Laboral, originado en el evento académico realizado en la Fundación Universitaria del Área Andina con el doctor Favio Farinella y en los trabajos que sobre el tema vienen realizando los estudiantes de la cátedra de investigación de la especialización en gerencia en seguridad y salud en el trabajo, de la sede Pereira.

Introducción

La capacidad laboral ofrece a las personas la posibilidad de mejorar su calidad de vida, mantener la salud y hacer uso de un derecho fundamental. Reynoso (2006) señala que el trabajo es trascendental en la vida económica, política y social, y requiere de la organización de leyes laborales que permiten regular las condiciones de trabajo. Azuela (2012) indica el principio y derecho fundamental irrebatible del trabajo como una condición inherente al ser humano, como tal, el trabajo constituye un derecho. De acuerdo con Mundlak (2007), existen tres componentes del derecho al trabajo, estos son: la libertad (la libertad de ejercer una profesión), el derecho a tener trabajo y la cuestionable obligatoriedad del Estado y los empleadores para proveer trabajo digno y bien remunerado a las personas.

A pesar de que los trabajadores representan cerca de dos terceras partes de la población mundial (OMS 2016), la crisis económica ha invisibilizado la importancia de sus derechos laborales en el contexto de los derechos humanos (Unesco 2014). Esta ponencia pretende llevar a empresarios, entes gubernamentales y estudiantes hacia una reflexión sobre el tema y su importancia en el fortalecimiento de la economía, ya que los cambios en cuanto a las políticas de cuidado de los trabajadores pueden lograr el desarrollo de economías más sólidas y rescatar el libre ejercicio de los derechos humanos (constitución política de Colombia, 1991). El tema es de alta relevancia para los especialistas en la materia, al igual que para los juristas (Colmenares, 2011).

Descripción de los temas

La OMS (2003, 2007) expone que muchos de los trabajadores del mundo carecen de salud y, por ende de salud laboral, una mínima parte de las personas que trabajan en el mundo, acceden a algún servicio de salud. En los sitios de trabajo y de manera continua existen riesgos y peligros como ruido, químicos, tóxicos, sustancias biológicas y maquinaria peligrosa, lo cual conlleva frecuentemente a una alta carga de enfermedades, discapacidades y muertes. Aunados a estos están los factores de riesgo laboral a nivel psicosocial, como el estrés y la violencia laboral, con alta representatividad en los países desarrollados y en constante aumento en los países en vías de desarrollo y en los países en transición (OMS, 2003).

Según la OIT (2017) "La protección del trabajador contra las enfermedades, sean o no profesionales, y contra los accidentes del trabajo" no es únicamente un derecho laboral, sino un derecho humano fundamental y uno de los principales objetivos de la OIT asignados por su Constitución. La contribución de la OIT al reconocimiento de los derechos humanos en el mundo del trabajo se refleja con claridad en los principios fundamentales de sus normas del trabajo, (OIT, 2009). La OIT trabaja desde sus inicios, a nivel mundial, a través de convenciones, tratados, pactos, declaraciones, convenios y recomendaciones, para lograr el cumplimiento de los derechos humanos en todo lo relacionado a los derechos laborales, entre los cuales cuenta la salud laboral de los trabajadores.

El respaldo de los gobiernos y las empresas para los trabajadores y el ejercicio de los derechos humanos en cuanto al trabajo, facilitan, en el trabajador, la calidad de vida en el trabajo y en el hogar y la sociedad. Un acondicionamiento asertivo en este tema provee de mejores condiciones de salud y económicas a todos los países del mundo, basados en condiciones mínimas fundamentales desde los derechos de las personas.

Hallazgos, contribución al área de conocimiento

Colombia, al igual que muchos países, presenta dificultades para el afrontamiento de una cobertura total en cuanto a la salud laboral, desde los derechos humanos, en los trabajadores de las empresas nacionales. La crisis económica, la politiquería, la irresponsabilidad gubernamental, al igual que la falta de compromiso de algunos empresarios han llevado a la expansión del trabajo informal, con incremento de riesgos, disminución de protección y pérdidas económicas y humanas representativas.

Conclusiones y limitaciones

A pesar de lo absurdo que parezca hablar del derecho a la salud laboral como derecho humano, es importante que tanto empresarios como instituciones jurídicas, provean de herramientas suficientes y completas a los trabajadores y sus representantes para la exigencia del cumplimiento de tales derechos, sin el reconocimiento gubernamental de los mismos, es difícil lograr los objetivos propuestos por la OIT.

Referencias

Azuela, H. S. (2012). *Tipología y estructura de los derechos humanos del trabajo*. Alegatos-Revista Jurídica de la Universidad Autónoma Metropolitana, 80, 7-26.

Colmenares, B. A. N. (2011). Los derechos laborales inespecíficos. Enfoque en el Derecho Venezolano. *Revista Latinoamericana de Derecho Social*, 13, 57-86.

Mundlak, G. (2007). Derecho al trabajo. Conjugar derechos humanos y política de empleo. *Revista Internacional del Trabajo*, 126 (3-4), 213- 242.

OIT (Organización Internacional del Trabajo) (2003b). Actividades normativas de la OIT en el ámbito de la seguridad y la salud en el trabajo: estudio detallado para la discusión con miras a la elaboración de un plan de acción de dichas actividades. Ginebra: Oficina Internacional del Trabajo.

OIT (Organización Internacional del Trabajo). (2006). *Convenio 187 sobre el marco promocional para la seguridad y salud en el trabajo*. Ginebra: Organización Internacional del Trabajo.

OIT (Organización Internacional del Trabajo). (2007). *Tiempo de trabajo decente. El equilibrio entre las necesidades del trabajador con las exigencias de los negocios.* Ginebra: Oficina Internacional del Trabajo.

OIT (Organización Internacional del Trabajo). (2010). *Constitución de la Organización Internacional del Trabajo y textos seleccionados.* Ginebra: Oficina Internacional del Trabajo.

OIT (Organización Internacional del Trabajo). (2011). *La igualdad en el trabajo: un objetivo que sigue pendiente de cumplirse.* Ginebra: Conferencia Internacional del Trabajo, 100 Reunión. Informe I (B).

OMS (Organización Mundial de la Salud). (1998). *Manual de instrucciones de la oms sobre calidad de vida.* Ginebra: Organización Mundial de la Salud.

OMS (Organización Mundial de la Salud). (2003). *El programa de salud ocupacional de la Oficina Central de la Organización Mundial de Salud (OMS)*. gohnet , 5 , 1-2.

OMS (Organización Mundial de la Salud). (2006). *Declaration on workers' health*. Italia: Organización Mundial de la Salud.

OMS (Organización Mundial de la Salud). (2007). *Salud de los trabajadores: proyecto de plan de acción mundial.* Ginebra: Organización Mundial de la Salud.

Pérez, J. P. (s. f.). *Derechos laborales: una mirada al derecho a la calidad de vida en el trabajo*. Ciencia Ergo Sum, 23(2), 121-133. Recuperado de http://www.redalyc.org/jatsRepo/104/10446094004/html/index.html

República de Colombia. *Constitución Política de Colombia*. Carta magna. 1991

Reynoso, C. C. (2006). *Derecho del trabajo, panorama y tendencias.* México: uam-Azcapotzalco.

Trejo Sánchez, Karina. (2013). La protección de la salud y la seguridad en el trabajo como derechos humanos. *El Cotidiano*, núm. 181, septiembre-octubre, 2013, pp. 81-90. Universidad Autónoma Metropolitana Unidad Azcapotzalco Distrito Federal, México

UNESCO (United Nations Educational, Scientific and Cultural Organization). (2008). *60 años de la Declaración Universal de Derechos Humanos.* Chile: Unesco para América Latina y el Caribe.

Derechos humanos y educación[1]

Nini Jhohanna Becerra González[2]

Fundación Universitaria del Área Andina - Colombia

Resumen

Establecer el punto de encuentro entre los conceptos de educación y derechos humanos no es una tarea compleja, pareciera casi una obviedad, pero toda la construcción teórica indica que no existe una dicotomía entre ambos. contrario a esto, existe una relación inquebrantable, ya que no es posible hablar de derechos humanos sin acudir a la educación como sistema que los valida, los enseña y los sostiene. De esta manera, el texto pretente generar una reflexión en torno a los desafíos de la educación para el abordaje de los derechos humanos.

Palabras clave

Derechos humanos, educación, instituciones educativas

[2] Licenciada en Pedagogía Infantil, Magíster en Educación desde la Diversidad, Especialista en Enseñanza de la Literatura, Especialista en Derechos Humanos y Doctorando en Ciencias de la Educación. Actualmente Docente de Posgrado de la Fundación Universitaria del Área Andina, Seccional Pereira, y directiva docente del sector oficial.
Correo institucional:
nibecerra@areandina.edu.co

1 Derechos Humanos y Discapacidad tiene su origen en el evento académico realizado en la Fundación Universitaria del Área Andina con el doctor Favio Farinella y en un trabajo de investigación previo como un aporte significativo a la defensa de los derechos y libertades fundamentales de los integrantes de la Policía Nacional de Colombia en situación de discapacidad.

Introducción

A pesar de la amplia construcción teórica, la correlación y la armonización de la educación y los derechos humanos en la vida cotidiana sí es una labor un tanto más ardua. De manera particular, formar en los derechos humanos en un país como Colombia tiene sus propias complejidades, entre ellas reconocer acontecimientos dolorosos, como crímenes de lesa humanidad, desapariciones forzosas, desplazamientos, niños con distintos desarraigos, asesinatos sistemáticos de líderes comunitarios, entre otros.

Lo anterior no solo es un panorama desolador, sino que se convierte en un verdadero desafío para los sistemas educativos. En este escenario surge necesariamente la obligación de re-pensar cuál es el papel de la escolaridad formal en la formación de sujetos vulnerados, pero al mismo tiempo de opresores, además de ello, debe pensarce cómo lograr que la escuela (desde el preescolar hasta el doctorado) haga el tránsito de lo teórico a lo práctico y, más interesante aún, cómo consolidar la escuela como institución social en un espacio que respete realmente los derechos de todos los actores partícipes en el bello acto de educar. Desde esta óptica, lo planteado es una invitación a refexionar sobre lo que sucede efectivamente en los sistemas educativos públicos y privados respecto al abordaje de los derechos humanos, con la finalidad de establecer los desafíos o retos propios de la enseñanza–aprendizaje de los mismos, en un mundo cada vez más globalizado, colapsado y hostil, es decir, cada vez menos humano.

Descripción de los temas, enfoque o perspectiva teórica del autor

Así las cosas, se podrían enunciar tres (3) posibles desafíos de la educación para abordar los derechos humanos al interior de sus instituciones formales: (I) la humanización de las propias instituciones educativas, (II) la transversalibilidad curricular y (III) la proyección social. Arriesgadamente, se podría indicar que una apuesta integral que logre reunir estos tres aspectos sería caminar con un paso más firme para construir la sociedad que se desea.

Ahora bien, sin duda alguna, para hablar de derechos humanos, la educación tendrá necesariamente que ser humanizadora, esto implica no asumir en su totalidad que es la solución a todos los problemas; al contrario, implica reconocer que la educación podría ser el problema, así como bien lo dijo Kafka: "*Creer en el progreso no significa creer que haya habido ya un progreso; eso no sería un acto de fe*". Por lo tanto, asumir la necesidad de la educación en el desarrollo de los derechos humanos no significa que esta haya alcanzado su máximo potencial en este ámbito.

> Uno oye decir continuamente que la solución de los problemas del mundo está en la educación. La tesis parece evidente, pero, ¿de qué educación hablamos? Hasta los funcionarios de la santa inquisición tenían métodos educativos, la Alemania nazi publicaba cartillas para entrenar el antisemitismo, hay escuelas de terroristas suicidas, hay modelos educativos hechos para perpetuar la discriminación racial, la exclusión social, hay academias que son reductos del espíritu aristocrático, semilleros de repulsión y de la rigidez mental, ¿Qué pasaría, si aún admitiendo que la educación es la solución de muchos problemas tuviéramos que aceptar que la educación, cierto tipo de educación, es también el problema? ¡Qué apasionante desafío para la inteligencia, no limitarnos a celebrar la educación en abstracto, sino exigirnos una nueva idea sobre lo que la educación debería ser! (Ospina, 2008, p, 192).

En consecuencia, el primer desafío consiste en hacer de la escuela un espacio de paz, de respeto, de reconocimiento de las diversidades, de equidad y de despliegue de las libertades, aspectos que están en sintonía con la Declaración Universal de Derechos Humanos (1948), al trazar el propósito de la educación en el sentido que:

> La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales; favorecerá la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos étnicos o religiosos; y promoverá el desarrollo de las actividades de las Naciones Unidas para el mantenimiento de la paz (art. 26).

Ahora bien, el segundo desafío acude a la didáctica y la necesidad de moverse del *saber- saber* al *saber-enseñable*, retomando lo que Yves Chevallard ha conceptualizado como transposición didáctica. Indiscutiblemente la enseñanza de los derechos humanos debe ser transversal y no una responsabilidad exclusiva de las ciencias sociales y, de manera opuesta, debe ser una tarea de todas las áreas del conocimiento y todos

los actores del sector educativo: directivos, docentes, administrativos, estudiantes y comunidad educativa en general.

Al respecto, Monclús y Sabán (1999) señalan que:

> El análisis de los temas transversales se encuentran en la actualidad en el centro de las discusiones educativas. Esta preocupación viene dada por las dificultades que provoca la puesta en práctica de nuevos diseños curriculares o de los desafíos didácticos referidos a la comprensión de fenómenos complejos o multidimensionales. Pero, sobre todo, destaca la necesidad de redefinir los contenidos socializadores (valores, normas, actitudes) que la escuela debe transmitir (p. 9).

Finalmente, el tercer desafío invita a girar la mirada hacia la extensión de la academia, mediante la proyección social y estar explícitamente contemplada en las misiones de las instituciones educativas, para ello se parte de dos (2) premisas claras: (I) el saber no circunda en las paredes de un lugar físico y (II) la educación tiene un compromiso con el entorno inmediato, al poner a disposición procesos y servicios, tales como los observatorios de políticas públicas, consultorios jurídicos, semilleros de investigación, entre otros.

Hallazgos, contribución al área de conocimiento

Colombia ha hecho esfuerzos que, sin ser suficientes, han tenido un impacto en la manera como se perciben y vivencian los derechos humanos; dichos empeños están basados en el propósito de una educación para todos y que promueva las competencias ciudadanas como uno de los anhelos de la sociedad. Lo anterior, se ve materializado en la cátedra de la paz, la cátedra de la afrocolombianidad y los proyectos tranversales que invitan al reconocimiento de las diversidades. Además, jurídicamente se han protegido los derechos humanos en las instituciones educativas mediante la creación de la Ley 1098 de 2006 por la cual se expide el código de la infancia y la adolescencia en Colombia, la Ley 1620 de 2013 por la cual se crea el sistema nacional de convivencia escolar y formación para el ejercicio de los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar, la cual se reglamenta con la aplicación del Decreto 1695 de 2013 y la Ley 1804 de 2016 por la cual se

establece la política de Estado para el Desarrollo Integral de la Primera Infancia de Cero a Siempre. Lo anterior, muestra un interés que se ha visto reflejado en la construcción de documentos jurídicos que apoyan y defienden los derechos humanos, en este sentido, la tarea de las instituciones educativas está direccionada hacia la generación de proyectos, programas y estrategias que garanticen el cumplimiento y veeduría de los mismos.

Conclusiones y limitaciones del capítulo

Si bien la escuela tiene un propósito de formación en competencias y aprendizajes, una de sus principales apuestas debería ser formar para la vida, si desea realmente apostarle al respeto de los derechos humanos, no para unos privilegiados sino como los derechos de todos. En este sentido, si la escuela es una de las más importantes instituciones sociales y, por tanto, la más indicada para enseñar a respetar la dignidad humana, deberá retomar la sensibilidad, la reflexión y la resistencia como caminos de emancipación frente a un orden que se impone y que desdibuja cada vez más la propia condición humana, la igualdad, la vida, la integridad y la libertad.

Referencias

Congreso de la República de Colombia. (2006). *Ley 1098 de 2006*. Colombia.

Congreso de la República de Colombia. (2013). *Ley 1620 de 2013*. Colombia.

Congreso de la República de Colombia. (2016). *Ley 1804 de 2016*. Colombia.

Congreso de la República de Colombia. (2016). *Decreto 1695 de 2013*. Colombia.

Organización de Naciones Unidas (1948). *Declaración Universal de Derechos Humanos*.

Ospina, W. (2008). *La escuela de la noche*. Grupo editorial Norma. Bogotá, Colombia.

Ministerio de Educación Nacional, Corporación Observatorio para la Paz, Fundación Universitaria del Área Andina. (2014). *Pacicultura para educación superior inclusiva*. Fundación Universitaria del Área Andina. Bogotá.

Monclús, A. y Sabán, C. (1999). *Educación para la paz*. Editorial Síntesis. Madrid, España.

Derechos humanos y discapacidad[1]

Alexander Antonio Rodríguez Valencia[2]

Fundación Universitaria del Área Andina - Colombia

[2]Abogado, Magíster en Derecho Público, Especialista en Pedagogía para la Docencia Universitaria y Especialista en Investigación Criminal. Docente de Posgrado en la Fundación Universitaria del Área Andina, Seccional Pereira.
Correo institucional:
arodriguez128@areandina.edu.co

Resumen

Si bien los derechos humanos, a partir de procesos de negociación, aprobación y ratificación de tratados internacionales, constituyen la piedra angular en la defensa de los derechos de las minorías –como son las personas en situación de discapacidad–, la realidad todavía da cuenta de un panorama de vulneración sistemática a las garantías mínimas de una población que, para la jurisprudencia de la Corte Constitucional colombiana, ha sido históricamente discriminada. Una de esas manifestaciones ocurre en una institución legendaria del Estado colombiano, como es la Policía Nacional "cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas" (C.P., art. 218), pero que desconoce los derechos de los policías que han adquirido algún tipo de discapacidad, optando por su no reubicación laboral, además de desconocer las obligaciones internacionales sobre la materia.

Palabras clave

Corte Constitucional, Derechos Humanos, Discapacidad, Policía Nacional, Reubicación Laboral, Tratados Internacionales

1 Derechos humanos y discapacidad tiene su origen en el evento académico realizado en la Fundación Universitaria del Área Andina con el doctor Favio Farinella y en un trabajo de investigación previo como un aporte significativo a la defensa de los derechos y libertades fundamentales de los integrantes de la Policía Nacional de Colombia en situación de discapacidad.

Introducción

En Colombia, los derechos de las personas con discapacidad, especialmente en materia de derechos fundamentales, adolecen de eficacia material, a pesar de los esfuerzos que desde mitad de siglo pasado hacia acá ha desplegado la sociedad internacional y los gobiernos democráticos del mundo por consolidar un numeroso marco normativo de declaración de derechos. Sin embargo, en el contexto práctico, las personas con discapacidad todavía deben soportar actitudes discriminatorias de quienes aún asocian el término discapacidad con incapacidad y que tiene una estrecha relación con un problema de inclusión social y que afecta igualmente a integrantes de la Policía Nacional. Desde esta perspectiva, asociar "derechos humanos y discapacidad" y la realidad que enfrentan los policías en situación de discapacidad, es un tema que trasciende las fronteras académicas y, en esa medida, debería ser el eje transversal de una política pública al interior de esa institución, en el marco de tratados internacionales de derechos humanos sobre la materia.

Descripción de los temas, enfoque o perspectiva teórica del autor

Desde la posguerra, los derechos humanos han alcanzado un elevado umbral de discusión en distintos escenarios, tanto a nivel académico, social y político, como al interior de las nacientes Organizaciones de Naciones Unidas (ONU) y Estados Americanos (OEA) que, a través de los procedimientos de negociación, adopción y ratificación de Tratados Internacionales, han vinculado a los gobiernos del mundo en su promoción y defensa.

Una primera manifestación tuvo lugar con la Declaración Universal de Derechos Humanos (1948) y el fin común que "los derechos humanos sean protegidos por un régimen de Derecho" (Preámbulo). En el escenario regional, con la Convención Americana de Derechos Humanos (1969), "reiterando que [...] sólo puede realizarse el ideal del ser humano libre si se crean condiciones que permitan a cada persona gozar de sus derechos [...]" (Preámbulo).

Bajo esta dinámica, también la discapacidad ha sido parte de la agenda internacional, a partir de instrumentos vinculantes para los gobiernos democráticos del mundo,

en este punto se resalta la Convención de los Derechos de las Personas con Discapacidad (2006), con el propósito de "promover, proteger y asegurar el goce pleno y en condiciones de igualdad de todos los derechos humanos y libertades fundamentales por todas las personas con discapacidad [...]" (art. 1).

El Tratado Internacional tiene una particularidad especial, basado en el reconocimiento que "la discapacidad es un concepto que evoluciona y que resulta de la interacción entre las personas con deficiencias y las barreras debidas a la actitud y al entorno que evitan su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás" (Preámbulo, lit. e), es decir, que la discapacidad ahora adquiere un enfoque de derechos humanos.

Lo anterior guarda coherencia con lo sostenido por Shakespeare (2013) sobre el modelo social de la discapacidad, en el entendido que "bajo este modelo, la discapacidad es una construcción social relacionada con la opresión social, el discurso cultural y las barreras en la sociedad", lo cual reafirma la tesis que la discapacidad no es enfermedad, ni tampoco justifica la exclusión social que por años ha padecido esta minoría en el mundo.

Hallazgos, contribución al área de conocimiento

En Colombia los derechos de las personas con discapacidad adolecen de eficacia material, en la medida que todavía deben soportar actitudes discriminatorias de quienes aún asocian el término discapacidad con incapacidad (Barboza, 2014), lo anterior, en el escenario menos hostil, tiene íntima relación con un problema de inclusión social que afecta directamente el desarrollo integral de esta población.

En ese contexto, la discapacidad no es un asunto que solo alberga a determinados sectores de la sociedad y, tal como se evidenció en una investigación adelantada en la Policía Metropolitana de Pereira (2016), algunos integrantes resultaron afectados en ejercicio de su deber constitucional (C.P., art. 218), un fenómeno que es comprensible si se considera la dinámica institucional de contrarrestar los factores que atentan contra la seguridad y la convivencia ciudadana. Es precisamente aquí donde convergen las normas internacionales de protección con una serie de situaciones que menoscaban el interés legítimo de los policías en situación de discapacidad y reubicación laboral, que su trabajo en esa institución tenga un mínimo de bienestar y respeto

a sus derechos humanos fundamentales, trasgredidos por la actitud, muchas veces discriminatoria de superiores y subalternos, poco tolerantes a aceptar la diferencia de sus compañeros.

En la actualidad, la situación de los policías con alguna limitación física o sensorial tiene connotaciones mucho más aberrantes, toda vez que hace carrera en los organismos médico-laborales, la práctica institucional de declarar la no aptitud para el servicio del servidor público con discapacidad y, coetáneamente, su no sugerencia de reubicación laboral, aspecto que agrava sus condiciones de estabilidad en el empleo y transgrede las normas supraconstitucionales.

Conclusiones y limitaciones del capítulo

Las personas en situación de discapacidad aún no han encontrado un escenario propicio para la materialización de sus derechos humanos fundamentales, no por falta de normas internacionales sobre la materia, que incluso tienen alcance supraconstitucional, sino porque en la práctica de las instituciones del Estado –como sucede en la Policía Nacional, por ejemplo–, los actos de discriminación recurrente evidencian un lamentable escenario de marginación laboral.

Referencias

Barboza, M. (2014). Acceso de las personas con discapacidad a los servicios públicos: derecho impostergable con base en el control difuso de convencionalidad. *Revista de Derecho Público de la Universidad de los Andes*, 14(32).

Colombia. Asamblea Nacional Constituyente. Constitución Política de Colombia de 1991

Colombia. Congreso de la República. Ley 1346 de 2009 "Por medio de la cual se aprueba la "Convención sobre los Derechos de las personas con Discapacidad". Diario Oficial No. 47.427 de julio 31.

Organización de Estados Americanos. (1969). *Convención Americana de Derechos Humanos.*

Organización de Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos.*

Organización de Naciones Unidas. (2006). Convención sobre los Derechos de las Personas con Discapacidad y su Protocolo Facultativo.

Rodríguez, A. (2016). *Reubicación laboral de integrantes de la Policía Nacional en condición de discapacidad en perspectiva con los derechos fundamentales y su alcance en la Justicia Constitucional: Estudio de Caso Policía Metropolitana de Pereira.*

Shakespeare, T. (2013). *The Social Model of Disability*. En DAVIS, Lennard J. (Ed.) The Disability Studies Reader, chapter 16. Fourth Edition. Routledge. Nueva York.

La auditoría médica y los derechos humanos[1]

Diego Carmona Carmona[2]

"La medicina es: la más humana de las artes, la más artística de las ciencias y la más científica de las humanidades".
Edmund Pellegrino

Resumen

En la atención en salud se deben tener en cuenta actividades asistenciales y actividades administrativas. Entre estas últimas, está la auditoría médica que hace parte de los procesos importantes en la atención de los usuarios a los servicios de salud ya que pretende asegurar que se cumplan los protocolos y se mantenga o mejore la calidad de los servicios prestados a los pacientes. La auditoría se apoya en los derechos humanos y la jurisprudencia existente el país para ofrecer a los usuarios todos los componentes de la calidad en el servicio, proyectando la atención sanitaria como una oportunidad de mejora en la calidad de vida de las personas.

Palabras clave

Auditoría médica, calidad en el servicio, atención en salud.

Fundación Universitaria del Área Andina - Colombia

[2] Médico y Cirujano. Especialista en Gerencia en Instituciones de Salud. Especialista en Auditoría en Salud, Maestrante en Administración de Hospitales y Servicios de Salud. Coordinador Académico de Dirección Seccional de Posgrados, Fundación Universitaria del Área Andina, Seccional Pereira.
Correo electrónico:
dcarmona@areandina.edu.co

3 Derechos Humanos y Salud Laboral, originado en el evento académico realizado en la Fundación Universitaria del Área Andina con el doctor Favio Farinella y en los trabajos que sobre el tema vienen realizando los estudiantes de la cátedra de investigación de la especialización en Gerencia en Seguridad y Salud en el Trabajo, de la sede Pereira.

Introducción

La auditoría médica está relacionada con la calidad y aplica los principios de Avedis Donavedian, y pretende determinar el nivel de calidad en la prestación de los servicios de salud. Para ello es necesario aplicar herramientas, que requieren recursos e infraestructura, todos enmarcados en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar, *W. Edwards Deming) con el fin de obtener resultados que conlleven a atención segura y que permitan la satisfacción de los pacientes y sus familiares. Para poder lograr estos aspectos es necesario que se tengan en cuenta distintas disciplinas que están interrelacionadas e implican aspectos éticos para respetar al ser humano en forma integral; y así lograr este objetivo, para ello se deben conocer los derechos humanos para evitar vulnerarlos durante el proceso de atención.

Descripción de los temas

En este relacionamiento entre los equipos de salud y los familiares y sus familiares, hay que tener en cuenta aspectos éticos, los cuales han sido tenido referenciados desde tiempos ancestrales que incluían entre otros el Juramento Hipocrático, en el cual se identifican varios principios que aún están vigentes y que, a pesar de intentar actualizarlos a la realidad actual, siguen teniendo vigencia y se hacen necesario para dictar lineamientos, generar reflexiones y permitan a que no se vulneren los derechos de los pacientes y así, respetar la integralidad del ser humano, incluyendo los derechos humanos intrínsecos al ser humano.

El código de ética de la "Mayo Clinic Foundation" incluye áreas como: ética, información confidencial y secretos propios de la organización, conflicto de intereses y actividades fuera de la institución, uso de los fondos y recursos de Mayo, relación con proveedores, libros archivos y documentos privados, actividad política y contribuciones, seguridad, salud y medio ambiente y relaciones entre el personal.

A través del tiempo, se han generado recomendaciones para mejorar la relación médico paciente, para conservar los principios éticos que incluyen que la relación sea respetuosa teniendo en cuenta algunos atributos de la calidad como la accesibilidad y la oportunidad, la comunicación adecuada, respetando el derecho que tiene el

paciente a estar informado de los hallazgos, conceptos, opiniones y mejores alternativas planteadas por los profesionales médicos, incluyendo la confidencialidad de la información depositada en la historia clínica.

También incluye que en dicha información este el paciente informado de las posibles consecuencias de cualquier acto médico, por medio de documentos como los consentimientos informados y las voluntades anticipadas, donde se respetan las necesidades y expectativas de los pacientes, incluyendo el disentimiento a cualquier actividad médica, investigativa o inclusive a maniobras que puedan prolongar su sufrimiento por actos que pudieran ser clasificados como encarnizamiento terapéutico y a una muerte digna, respetando los principios culturales, morales y religiosos. Otros derechos que se deben respetar son la privacidad, confidencialidad, pertinencia, integralidad, continuidad, humanización y seguridad en la atención para evitar la maleficencia en la atención, con personal autorizado legalmente para prestar los servicios de salud. Tienen derecho a recibir segundos conceptos o ser remitidos a niveles superiores en caso de requerirlos.

Hallazgos y aportes

El Ministerio de Salud y la Protección Social ha implementado herramientas para hacer respetar los derechos de los pacientes que incluyen la Política de Seguridad del Paciente y la Política de Humanización por medio de las cuales se cuentan con elementos estructurales, procesos, instrumentos y metodologías basadas en evidencias científicamente probadas que propenden por minimizar el riesgo de sufrir un evento adverso en el proceso de atención de salud o de mitigar sus consecuencias. Implica la evaluación permanente de los riesgos asociados a la atención en salud para diseñar e implantar las barreras de seguridad necesarias.

Conclusiones

Los derechos humanos deben ser respetados en todos los ámbitos donde los seres humanos se relacionan e involucran, incluyendo la relación médico paciente. La auditoría médica debe velar por que se respeten estos derechos y se evite vulnerarlos por medio de herramientas y mecanismos que sean aplicados previos, durante y posteriores a la atención médica. En el caso de la seguridad del paciente, es posible que

se presenten eventos adversos, los cuales implican el daño del paciente durante el proceso de atención, pero teniendo en cuenta que por definición es involuntario, lo que se debe hacer es ser transparente e informarle al paciente el evento presentado, hace un compromiso y las acciones de mejoramiento para evitar que se repita y tratar de subsanar el daño presentado.

Derechos humanos y tecnología

(Los ciberataques y el uso de la fuerza en el derecho internacional)

Favio Farinella[1]

Resumen

La responsabilidad internacional del Estado continúa siendo una temática en construcción, máxime en la intersección entre los derechos de la persona humana y eventuales conflictos nacidos a partir del uso de las nuevas tecnologías de la información y la comunicación. En este punto nace el siguiente interrogante: ¿Hasta qué punto el derecho internacional es apto para enfrentar actividades que eventualmente implican el uso de la fuerza a través de la utilización de las nuevas tecnologías? El presente trabajo se centra en analizar dos cuestiones nacidas de la relación entre los derechos humanos y las ciberoperaciones. Por un lado, se intentarán evaluar los posibles límites legales a las operaciones cibernéticas que afectan derechos básicos; y por otro, conocer las dificultades que se presentan al momento de interpretar y aplicar el derecho internacional a los ciberataques. En lo específico, se dará respuesta a tres interrogantes, donde se pretender conocer bajo cuáles circunstancias, un ciberataque puede (I) constituir una amenaza o uso ilícito de la fuerza; y entonces (II) justificar la legítima defensa individual o colectiva; y finalmente (III) cuáles reglas del derecho internacional humanitario pueden aplicarse a los ciberconflictos.

Palabras clave

Ciberataques / derecho internacional humanitario / legítima defensa / uso de la fuerza

Fundación Universitaria del Área Andina - Colombia

[1] PhD. Profesor, investigador. UNMdP, UAI. BSc. in International Relations and Politics, University of London, Ex Becario Seoul National University, Comisión Europea Programa Marie Curie y TMC Asser Institute. Contacto: faviofarinella@hotmail.com. Especial para la Fundación Universitaria del Área Andina. Octubre de 2018.

Introducción a los conceptos básicos utilizados

Todo sistema legal provee consecuencias frente a la violación de sus normas. El Derecho Internacional (DI de aquí en más) no es la excepción. No obstante, constituye un conjunto de normas particulares, donde la voluntad de los Estados soberanos continúa siendo determinante al momento de brindar eficacia al derecho vigente. La irrupción de las Nuevas Tecnologías de la Información y Comunicación (NTIC en adelante) plantea preguntas inéditas para el campo del derecho y de las relaciones internacionales. La evolución del DI marcada por cuestiones vitales como la paz, la guerra y el dominio territorial del Estado clásico vuelve a presentarse bajo un matiz nunca antes conocido: el del ciberespacio. En este ámbito intangible y sin titulares precisos, las nociones de cooperación y conflicto se encuentran y, además, reclaman respuestas.

En este artículo se propone debatir las posibles interacciones jurídicas de un tipo especial de uso que puede darse a las NTIC: los cibertaques. La utilización de las NTIC con fines bélicos demanda nuevas respuestas a conceptos tradicionales del DI. Entre todas, se elige contestar aquí las siguientes: (I) ¿se enmarca un ciberataque en el concepto de uso prohibido de la fuerza conforme el artículo 2(4) de la Carta ONU?; (II) si así fuera, ¿puede entonces el Estado lesionado ejercer su derecho de legítima defensa conforme el artículo 51 de la Carta?; y (III) ¿es posible aplicar a los ciberataques las reglas y principios del Derecho Internacional Humanitario?

El ciberespacio es el único lugar enteramente creado, mantenido, poseído y administrado por el hombre, sean ya prestadores públicos o privados. Puede ser definido como una red globalmente interconectada de información digital e infraestructura de la comunicación, que incluye Internet, redes de telecomunicaciones y sistemas de computación, junto con la información que reside en ellos[2]. Su característica distintiva es el cambio constante como respuesta a la innovación tecnológica. Concebido

2 Para otra definición de ciberespacio ver *The White House, Cyberspace Policy Review*, 16 May 2011, p. 1, en referencia a la Directiva Presidencial Estadounidense de Seguridad Nacional 54 / *Homeland Security Presidential Directive* 23 (NSPD-54/HSPD23): *"the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"*.

como un lugar para el desarrollo de las comunicaciones y la actividad económica pública y privada, jamás se pensó que las reglas del Derecho Internacional Humanitario (DIH en adelante) le fueran aplicables. Los datos e información viajan en forma de múltiples fragmentos digitalizados a través de rutas absolutamente impredecibles antes de ser reconstituidos en el lugar de destino.

Como el ciberespacio se encuentra accesible a los gobiernos, organizaciones no estatales, empresas privadas e individuos por igual, las direcciones IP simuladas (IP spoofing)[3] y el uso de redes de robots informáticos hacen sencillo disfrazar el origen de una operación a fin de no ligar el resultado dañoso con el verdadero atacante, con lo cual se evita la prueba del nexo causal, vital al momento de discutir la responsabilidad legal sobreviniente.

Frente a esta situación, la seguridad del ciberespacio se vuelve un tema determinante. Según el Manual de Tallin sobre el DI aplicable a las ciberoperaciones[4], el término ciberseguridad comprende la protección de la confidencialidad, integridad y disponibilidad en el ciberespacio, así como los servicios de computación y las redes, la maquinaria (hardware) y la información y contenidos[5]. Por su parte, la definición de la Unión Internacional de Telecomunicaciones dispone que la ciberseguridad es la colección de herramientas, políticas, conceptos y herramientas de seguridad, protocolos y guías de seguridad, acciones, entrenamiento, mejores prácticas, asegurabilidad y tecnologías que pueden utilizarse para proteger el ciberespacio y los bienes de la organización y de las personas. Dentro de estos se incluye al hardware, la infraestructura, el personal, las aplicaciones los servicios y los sistemas de telecomunicación y la totalidad de la información transmitida y almacenada en el ciberespacio[6].

3 Tanto la suplantación de IP (Protocolos de Internet) consiste en crear paquetes de IP a fin de sustituir una o más direcciones del IP original (TCP/IP) al cual se desea suplantar por otra dirección IP. Esto se consigue generalmente gracias a programas destinados a ello y el objetivo es volver más dificultoso o directamente imposible rastrear el destinatario.

4 El Manual de Tallinn (Tallinn Manual on the International Law Applicable to Cyber Warfare) es un estudio académico no vinculante sobre el DI (el jus ad bellum y el DIH) aplicable a los ciberconflictos y los ciberataques. Entre 2009 y 2012, el Manual fue escrito a invitación del Tallinn - based NATO Cooperative Cyber Defence Centre of Excellence por un grupo de aproximadamente 20 expertos internacionales. En Abril de 2013, el Manual fue publicado por Cambridge University Press.

5 Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional (International Organization for Standardization and International Electrotechnical Commission). Documento ISO/IEC 27032 (2012). Information technology. Security techniques. Guidelines for cybersecurity.

6 International Telecommunication Union. ITU Publications X.1205 : Overview of cybersecurity (2008).

Cada Estado dentro de su jurisdicción tiene la obligación de proteger a su población de todo delito, incluidos los llamados delitos informáticos, tales como el espionaje en Internet, el robo de secretos, la privacidad e intimidad y la información financiera. La ciberseguridad abarca la totalidad del proceso por el cual los archivos de datos e información se encuentran en tránsito, son procesados y finalmente almacenados.

La Relatoría Especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos, estableció en su publicación *Libertad de expresión e Internet* respecto de la ciberseguridad:

> El concepto de ciberseguridad suele emplearse como un término amplio para referirse a diversos temas desde la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de Internet, hasta la seguridad o integridad de los usuarios. No obstante, desarrollos posteriores sugieren la necesidad de limitar el concepto exclusivamente al resguardo de los sistemas y datos informáticos (…) este enfoque acotado permite una mejor compresión del problema así como una adecuada identificación de las soluciones necesarias para proteger las redes interdependientes y la infraestructura de la información (OEA, 2013).

Cuando la ciberseguridad falla, cobra importancia la conducta del agente que la provoca. Si el ataque es masivo y afecta a la población de un Estado, a través de la degradación o prohibición de uso de servicios y contenidos gubernamentales o privados, posiblemente se está frente a un ciberataque. Por ciberataque se entiende todo esfuerzo realizado para alterar, desviar, degradar o destruir los sistemas operativos de las computadoras o redes o la información o programas en ellas existentes[7]. Todo ciberataque es conducido a través del ciberespacio y utilizando sus herramientas. Solo a modo de ejemplo, la infección de un sistema de redes de computadoras con un virus maligno podría constituir un acto de ciberataque, como el caso del gusano Stuxnet referido más adelante. Los objetivos de un ciberataque pueden incluir la vida de personas o la funcionalidad de objetos que dependan de los sistemas de computación atacados. Por ejemplo, los casos de estaciones de energía, medios de transporte

7 Esta definición se basa en la utilizada por el Comité del Consejo de Investigación Nacional sobre Guerra de Información Ofensiva en Tecnología, Política, Derecho y Ética respecto de la adquisición y uso por parte de Estados Unidos de capacidades orientadas al ciberataque. Ver Owens, William A., Dam, Kenneth W. y Lin, Herbert S. (eds.), (2009), conocido como NRC Committee Report.

o personas conectadas a varios tipos de sistemas de soporte de vida médico, militar o profesional.

Un ciberataque puede estar dirigido a atacar, explotar o defender una red informática[8], pues comprende todo tipo de ciberoperaciones que tengan por fin "interrumpir, negar, degradar o destruir la información residente en computadoras y redes informáticas o las computadoras y las redes en si mismas" (OEA, 2013).

Potenciales consecuencias de un ciberataque

Las capacidades ofensivas de los ciberataques son tales que pueden paralizar la administración del Estado atacado, o los sistemas operativos de privados que prestan servicios públicos. Por ejemplo, las redes de defensa militar de un Estado pueden ser desactivadas o degradadas en forma remota. De igual manera, al inundar con pedidos de información un sitio de Internet, un servidor o un router se recarga su capacidad de funcionamiento y se provoca la llamada 'denegación de servicio'. Su efecto es hacer caer las redes informáticas de cualquier Estado que utilice comunicaciones por Internet. También las redes del sector privado pueden ser infiltradas, dañadas o destruidas[9]. En el sentido que se comenta, los efectos de un ciberataque comparten semejanzas tanto con la fuerza militar cinética, como con la coerción económica y la subversión, aunque poseen características propias que evolucionan rápidamente[10].

Los antecedentes de ciberataques son tan pocos como preocupantes, no solo porque involucran paradigmas básicos de las relaciones internacionales como la guerra y la paz, sino porque además la actual sociedad digital se define a sí misma por el uso constante y creciente de las NTIC. El estado de derecho y el respeto por los derechos humanos moldean sus aristas digitales, como el voto electrónico, las redes

8 EEUU, Departamento de Defensa, The National Military Strategy for Cyberspace Operations, (2006).

9 Comunicado de Prensa, Chipman, John, Director-General of the International Institute for Strategic Studies, The Military Balance 2010 (03/02/2010). Disponible en http://wwws.iiss.org/publications/ military-balance/ the- military- balance- 2010/military-balance-2010 -press- statement/ .

10 Un ataque cinético es el acto de atacar desde el espacio una parte de la superficie planetaria con un proyectil no explosivo donde la fuerza destructiva proviene de la energía liberada durante el impacto del proyectil. Su antecedente fueron las máquinas de asedio que disparaban piedras.

sociales y la digitalización de procedimientos que hacen efectivo el respeto de los derechos. Incidir de manera intencional a fin de degradar o destruir el ciberespacio donde se almacenan información y contenidos, implica un grave atentado contra la legitimidad de la democracia y el ejercicio efectivo de los derechos humanos y -como se verá- una potencial amenaza a la paz y seguridad internacionales.

En 1988 se registra el primer "gusano" reconocido por haber afectado la incipiente infraestructura cibernética del mundo. El gusano Morris se extendió a gran cantidad de computadoras en los Estados Unidos, ralentizándolas al punto de volverlas inutilizables[11] . Diez años después, en 1998, se registra el primer ciberataque masivo de la historia cuando más de 3000 hackers 'privados' atacaron desde China los servidores que albergaban sitios gubernamentales de Indonesia[12]. No obstante, es en 2007 cuando el problema escala a nivel planetario. El 27 de abril de 2007 el gobierno Estonio decide retirar una estatua de bronce del centro de su capital Tallin, que había sido erigida en 1947 para conmemorar a los soldados Soviéticos caídos en la Segunda Guerra Mundial, a fin de reubicarla en un cementerio militar. Rusia advirtió que la decisión tendría consecuencias desastrosas. Días después, hackers nunca identificados, atacaron sitios gubernamentales y privados del Estado Estonio. A partir de ese momento, los habitantes de Estonia no pudieron acceder a ningún sitio gubernamental, pero tampoco a medios de comunicación, ni sitios académicos como universidades o escuelas, ni a los bancos. Sin saberlo, Estonia se hallaba frente al primer ciberataque a escala masiva dirigido contra toda la infraestructura de NTIC de un Estado soberano. En ese momento, Estonia reaccionó y calificó la situación como un estado de ciberguerra, comparándolo con el bloqueo de puertos o ciudades, típico de la estrategia militar de otros siglos. Es importante también mencionar que nunca pudo comprobarse que la Federación Rusa hubiera estado involucrada en el hackeo.

11 Fue obra de Robert Tapan Morris, quien alegó estar tratando de medir la magnitud de Internet. Morris se constituyó en el primer condenado bajo la ley Estadounidense de fraude y abuso de computadoras, aunque ahora es profesor del MIT. Para un relato cronológico completo de la historia de los ciberataques, véase la revista de la *OTAN, NATO Review* disponible en https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm (agosto de 2018).

12 Esos grupos son conocidos por todos los servicios de inteligencia de Occidente. *Red Hackers of China, China Eagle Union, Green Army Corps o Honkers Union of China* constituyen núcleos de piratas informáticos etiquetados como "defensores de la dignidad y la integridad de la patria". El Partido Comunista Chino se muestra tolerante al punto de instrumentalizarlos. Desde principios del año 2000, Estados Unidos denominó con el código de Titan Rain al conjunto de esos ciberataques orquestados desde China. Los grupos de hackers se componen de jóvenes investigadores, ingenieros informáticos y profesionales nacionalistas ligados a las NTIC.

La respuesta, tal como si hubiera sobrevenido un ataque armado en contra de un país miembro de un esquema de seguridad colectiva, fue inmediata. La Organización del Tratado del Atlántico Norte (OTAN en adelante), estableció una unidad de Defensa de Internet en Estonia, lo cual derivó en que en 2018 este Estado se convirtiera en el primer gobierno digital del mundo[13]. Precisamente, el mayor estudio existente sobre el DI aplicable a todo tipo de ciberoperaciones incluidos los ciberataques fue realizado en Tallín, cuando a instancias de la OTAN un grupo de expertos internacionales redactó el *Manual de Tallín sobre el DI aplicable a las ciberoperaciones* (2013).

Durante el conflicto entre Georgia y la Federación Rusa por la región de Osetia del Sur en 2008, se produjo el primer uso de Internet como arma de guerra. Mientras transcurría el conflicto armado, Rusia inició ataques de denegación de servicio (*DDoS distributed denial of service*) sobre sitios del gobierno Georgiano, medios de comunicación y sitios comerciales. El ataque duró un mes y aunque la disrupción de servicios fue leve, los hackers lograron presionar al gobierno Georgiano de manera coordinada con las acciones militares rusas.

En un artículo publicado en 2010, el Secretario de Defensa de Estados Unidos reveló que en 2008 el Departamento de Defensa había sufrido "la más significativa violación de computadoras militares de Estados Unidos en su historia" (William J., 2010, p. 98), cuando un pendrive insertado en una laptop de uso militar introdujo software malicioso en el sistema de computadoras clasificado y desclasificado del Comando Central de Estados Unidos. Desde entonces, los Estados Unidos se ocuparon de desarrollar sistemas defensivos dirigidos a proteger la infraestructura electrónica, militar y civil, de intrusiones y potencialmente peor, disrupciones y destrucción, todo lo cual constituye hoy la ciberestrategia de defensa de Estados Unidos en la era digital.

Durante 2009 y 2010 el gusano Stuxnet infectó computadoras de Siemens utilizadas en el programa nuclear Iraní. Se cree que el gusano fue creado por Estados

13 El 99 % de los trámites oficiales pueden realizarse durante las 24 horas, los siete días de la semana. Así, sus ciudadanos pueden revisar redes sociales, hacer la compra semanal de comida, pero también renovar su pasaporte, firmar un documento o crear una empresa. El papel desapareció de las reuniones del Consejo de Ministros en el año 2000. Los Estonios solo necesitan una conexión a Internet para votar, renovar su carnet de conducir, consultar recetas médicas, presentar reclamaciones por importes menores a 2.000 euros, hacer la declaración de ganancias, impugnar una multa de tránsito, cambiar su domicilio, registrar una empresa, firmar documentos, ver las notas de sus hijos y comunicarse con profesores o acceder a su historial médico. Ver El Pais, en internet https://elpais.com/elpais/2018/04/05/eps/1522927807_984041.html disponible en agosto de 2018.

Unidos con la participación de Israel y de la misma Siemens con el objeto de demorar durante años el programa. Al aumentar la velocidad de los motores centrífugos más allá de lo necesario, produjo errores que demoraron los avances Iraníes. Stuxnet afectó luego a India, Indonesia y a la Federación Rusa. Su importancia histórica radica en haber sido el primer gusano diseñado con el objetivo de afectar la infraestructura del mundo real, como podrían serlo estaciones de energía, plantas potabilizadoras o industrias.

En enero de 2010, un grupo llamado Ciber Ejército Iraní degradó el servicio del buscador Chino más popular (Baidu) para redirigir toda consulta hacia una página con mensajes políticos iraníes.

En enero de 2011, Canadá reportó haber sido víctima de un ciberataque masivo en contra de sus agencias gubernamentales, donde también se encontraba el Departamento de Defensa Nacional. Por esto, debió bajar los sitios del departamento de Finanzas y del Tesoro Canadiense.

En Junio de 2013, la OTAN dedica su primera reunión de la historia a la Ciberdefensa. En ella, los Ministros de Defensa de los países miembros acordaron que las capacidades ciber-defensivas de la Alianza deberían encontrarse completamente operacionales para mediados de ese año y se extendió la protección a todas las redes de titularidad u operadas por la Alianza, independientemente del territorio donde se encuentren.

En junio de 2016, *The Washington Post* revela que la inteligencia Rusa había hackeado los servidores del partido Demócrata con la intención de robar datos comprometedores sobre el presidente Trump. De comprobarse, se estaria frente a una situación en la que un Estado extranjero interfiere en el resultado de elecciones de un Estado democrático.

Finalmente, a mediados de Julio de 2016 el Secretario general de la OTAN anuncia que la Alianza militar comienza a reconocer al ciberespacio como un dominio operacional de conflicto, de igual manera que el aire, el mar y la tierra. Afirma, además, que algunos ciberataques pueden dar lugar a la legítima defensa colectiva.

Uso legal de la fuerza en las relaciones internacionales

Los redactores de la Carta ONU tuvieron dos objetivos claros respecto del uso de la fuerza: (I) prohibir el uso unilateral; y (II) centralizar su control en el Consejo de Seguridad ONU (CS en adelante).

El artículo 2(4) de la Carta ONU refleja ciertos principios fundantes sobre los cuales descansa la paz y seguridad internacional y el sistema de seguridad colectiva. La regla general que afirma es la prohibición de la amenaza y del uso de la fuerza. Existen tres excepciones básicas: (I) la legítima defensa; (II) la autorización brindada por el CS en el marco del Capítulo VII de la Carta; y (III) el ejercicio del derecho a la libre determinación de los pueblos.

- Primero y en relación con la legítima defensa, el artículo 51 de la Carta ONU afirma que "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas (…)". El aporte del DI consuetudinario en la cuestión se expresa través de ciertas Resoluciones de la Asamblea General ONU (AG en adelante): (I) la definición de la Agresión (Res. AG 3314 de 1974); (II) la declaración relativa a los Principios de DI referentes a las Relaciones de Amistad y Cooperación entre Estados (Res. AG 2625 de 1970); y (III) la declaración sobre el mejoramiento de la eficacia del Principio de abstención de la amenaza o de la utilización de la fuerza en las relaciones internacionales (Res. AG 42/22 de 1988).

- Segundo, el artículo 42 de la Carta ONU faculta al CS a decidir las acciones necesarias -incluido el uso de la fuerza- a fin de mantener o restablecer la paz y la seguridad internacionales.

- Tercero, el derecho a la autodeterminación se encuentra en importantes documentos universales, tales como ambos Pactos Internacionales de Derechos Civiles y Políticos y de Derechos Económicos, Sociales y Culturales[14]. La Resolución de la AG 1514 (XV) convierte el principio en derecho, en tanto la Resolución AG 2625 (XXV) desarrolla los derechos y obligaciones emergentes.

14 AG ONU, Resolución 2200 A, 16/12/1966.

Más allá de las tres excepciones referidas, existen amplias zonas grises respecto de la legalidad de la amenaza y uso de la fuerza. En ellas la controversia es la regla.

Las resoluciones de la AG antes referidas fueron adoptadas por consenso, lo que implica por defecto, que varias de las cuestiones controvertidas recibieron una redacción ambigua y continúan latentes. Por ejemplo, respecto de la extensión del uso legal de la fuerza en el sistema internacional, permanece el debate entre una concepción estricta y otra amplia. Mientras Estados Unidos, Israel o Francia se inclinan a defender a sus nacionales en el exterior incluso militarmente y hablan de la autodefensa preventiva, la mayoría de los Estados rechazaban estas posiciones al menos hasta antes del 11/09.

Una segunda cuestión controvertida y latente es la calificación de "fuerza" que algunos identifican exclusivamente con fuerza armada. Otros optan por incluir situaciones de dominación o coacción no armada. La consecuencia es relevante, ya que el uso ilegal de la fuerza habilita -para quienes apoyan una concepción amplia-, el ejercicio del derecho a la autodeterminación.

Una tercera controversia es la relativa a la legalidad de la amenaza o uso de las armas nucleares. Además, se generan continuamente opiniones dispares respecto a su calificación como uso de la fuerza, las cuestiones referidas a bloqueos económicos o la degradación o contaminación ambiental como herramienta utilizada durante un conflicto armado. A estas cuestiones no resueltas, se agrega la que motiva este artículo: los ciberataques.

A continuación se analizan las tres hipótesis planteadas al inicio:

1. **¿Se enmarca un ciberataque en el concepto de uso prohibido de la fuerza conforme el artículo 2(4) de la Carta ONU?**

La utilización de las NTIC en conflictos presenta desafíos especiales para la regulación legal internacional, debido a que sus características difícilmente encuadran en los mecanismos de aplicación y denuncias tradicionales, como el Consejo de Seguridad de Naciones Unidas, o evaluaciones descentralizadas a cargo de Estados, organizaciones internacionales y otros actores internacionalmente relevantes[15]. Comenta el Profesor Dinstein respecto de los ciberataques:

15 Ver Oscar Schachter, The Right of States to Use Armed Force, 82 Michigan Law Review 1620, ps. 1645-46 (1984).

> La novedad de un arma siempre desconcierta a estadistas y abogados, muchos de los cuales quedan perplejos ante la innovación tecnológica (...) Tras el período de gestación, las partes beligerantes entienden que no existe una dificultad insuperable en aplicar los principios generales del Derecho Internacional a la nueva arma (Michael N. Schmitt y Brian T. O'Donnell, 2002, p. 114).

Los trabajos preparatorios de la Carta ONU evidencian que sus redactores entendían que la prohibición del uso de la fuerza no debía ser extendida a situaciones como: presiones políticas o coerción económica[16]. Esta concepción podría incluir hoy a las ciberoperaciones ofensivas y defensivas. La mayor parte de la doctrina considera que el término fuerza conforme el articulo 2(4) de la Carta ONU es sinónimo de fuerza armada o militar[17]. No obstante, se cree que si la consecuencia de un ciberataque se traduce en la muerte o daños a personas o la destrucción de objetos e infraestructura, la respuesta puede cambiar[18]. En cuanto a lo que debe entenderse por 'amenaza' y en tanto la Carta ONU no define lo que constituye una amenaza ilícita de la fuerza interestatal, la CIJ (1996) sostuvo que:

> Las nociones de amenaza y uso de la fuerza bajo el artículo 2, parágrafo 4 de la Carta se encuentran unidos en el sentido que si el uso de la fuerza en un caso dado es ilegal -por la razón que sea-, la amenaza de usar dicha fuerza también será ilegal. En resumen, para ser legal, la voluntad declarada de un Estado a fin de utilizar la fuerza en carácter de legítima defensa, debe hallarse en conformidad con la Carta ONU (p. 47).

Un primer obstáculo a sortear en los ciberataques es la prueba. La imputación de responsabilidad conforme la prueba obtenida es relevante no solo a fin de imponer sanciones, sino en caso que el Estado atacado decida ejercer su derecho de autode-

16 La propuesta Brasilera de extender la prohibición a la "amenaza o el uso de medidas económicas de cualquier forma inconsistente con los propósitos de las Naciones Unidas" fue rechazada por la Conferencia de San Francisco. Documentos de la Conferencia de Naciones Unidas sobre la Organización Internacional, vol. VI (1945), pp. 559; 720–721.

17 Ver Randelzhofer, Albrecht, Article 2(4), en Bruno Simma (ed.), The Charter of the United Nations: A Commentary, vol. I (2002), p. 117. Igualmente Dinstein Yoram, War, Aggression and Self-Defence, 4a. ed. (2005), p. 81; Brownlie Ian, International Law and the Use of Force by States, (1963), pp. 362; 431.

18 Ver Tallinn Manual on the International Law Applicable to Cyber Warfare, Schmitt, Michael N (Gen. ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press.

fensa. Las ciberoperaciones auspiciadas por un Estado que calificaran como uso de la fuerza contra otro Estado no solo violarían la prohibición general del 2(4) de la Carta ONU, sino que podrían desatar un conflicto armado internacional.

La existencia de una violación al artículo 2(4) basada en el uso de las NTIC es extremadamente difícil de obtener y/o verificar. Mientras que, respecto de un ataque realizado a través de un misil, es posible conocer la dirección de envío, un virus que afecta computadoras no es trazable. El trabajo forense necesario para identificar a un ciberatacante puede tomar meses, o ser directamente imposible. Como los conflictos subrogados de la guerra fría, pero con una extensión mayor, las ciberoperaciones dan lugar a una amplia discusión respecto de cuáles han sido los hechos realmente sucedidos, donde además se incluye quién cometió la intrusión o disrupción y en nombre de quién fue realizada.

Una segunda cuestión es la relativa a la licitud de los cibertaques y su relación con la prohibición del uso de la fuerza. La eventual ilicitud de un ciberataque no implica a priori que constituya una amenaza o uso de la fuerza prohibidos por el DI.

La ilegalidad de una ciberoperación puede resultar de la violación de cualquier obligación impuesta al Estado por el DI general. Por ejemplo, el DI general prohíbe la explotación de sistemas informáticos con el propósito de recolectar información sin consentimiento de los titulares; también la difusión de propaganda hostil o la propagación de *fake news* a fin de direccionar a la opinión pública hacia determinada decisión; o la realización de ataques dirigidos a suspender el servicio de Internet. Todos estos supuestos violarían la soberanía del Estado afectado y eventualmente el principio de no intervención, aun cuando tales situaciones no alcanzaran *per se* a ser calificadas como uso de la fuerza conforme la interpretación mencionada del articulo 2(4) de la Carta ONU[19].

19 Conforme la "Declaración sobre la inadmisibilidad de la Intervención e Interferencia en los Asuntos internos de los Estados" anexa a la Resolución 36/103 de la AG ONU de fecha 09/12/1981, el principio de no intervención incluye, inter alia, los siguientes derechos y deberes: I (c) el derecho de los Estados y pueblos a tener libre acceso a la información y a desarrollar en forma completa sin interferencia, sus sistemas de información y medios de comunicación y utilizar la información mediática a fin de promover sus intereses y aspiraciones políticas, sociales, económicas y culturales, basadas entre otros en los artículos relevantes de la Declaración Universal de Derechos Humanos y los principios del nuevo orden de la información internacional; II (j) el deber del Estado de abstenerse de campañas difamatorias, o propagando hostil o vil con el propósito de intervenir o interferir en los asuntos internos de otros Estados; III (d) el derecho y deber de los Estados de combatir dentro de sus prerrogativas constitucionales, la propagación de noticias falsas o distorsionadas que puedan ser interpretadas como una interferencia en los asuntos internos de los Estados o ser perjudiciales para la promoción de la paz, la cooperación y las relaciones de amistad entre Estados y naciones.

En forma similar, las ciberoperaciones que no implican como resultado una destrucción física sino solo intrusiones en el sistema de archivos del Estado afectado, o bien la correspondencia y documentación de una misión diplomática extranjera, o interfirieran con la libertad de comunicación de la misión diplomática, violarían obligaciones internacionales impuestas al Estado receptor conforme el DI general sin llegar a constituir actos de amenaza o uso de la fuerza[20]. En la misma línea, otras afectaciones de derechos pueden presentarse a partir de ciberataques y ser potencialmente relevantes a la luz del comercio internacional o de los derechos humanos, cuando por ejemplo, los ataques interfieren con la libertad de comercio o la libertad de información, pensamiento y expresión [21]. En los casos mencionados, los ciberataques son ilegales y generan responsabilidad internacional, aun cuando prima facie, no constituyen amenaza o uso de la fuerza que habilite la autodefensa.

Frente a los diversos tipos de daño que puede producir un ciberataque, se entiende que tanto su caracterización como el derecho aplicable deben analizarse en función de los efectos producidos. Una ciberoperación puede estar dirigida a manipular sistemas informáticos estatales o no, a fin de causar el colapso de una planta de energía nuclear, o la apertura de compuertas de una represa cercana a un área densamente poblada, o la deshabilitación del control de tráfico aéreo en un aeropuerto congestionado vigentes malas condiciones climáticas. En cada uno de estos ejemplos, las consecuencias pueden medirse en términos de muertes, daños y destrucción.

A pesar de aceptar la concepción restrictiva que identifica el uso de la fuerza con la fuerza armada o militar, esto no significa necesariamente que la prohibición se limite a la utilización de armamento cinético, químico, biológico o nuclear, y deba descar-

20 Convención de Viena sobre Relaciones Diplomáticas, arts. 24, 27 y 45(a).

21 Conforme el artículo 19 de la Declaración Universal de los Derechos Humanos, "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión". De igual manera, el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos declara: 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas."

tarse el uso de las NTIC. Conforme la Corte Internacional de Justicia (CIJ en adelante), la prohibición del artículo 2(4) de la Carta ONU (1996) se aplica a "cualquier uso de la fuerza, sin que importe el armamento empleado" (parágrafo 39)[22].

En el caso Actividades Militares y Paramilitares en Nicaragua, la CIJ distinguió las formas más graves del uso de la fuerza, de otras violaciones menores. No obstante, afirmó que incluso actos de fuerza interestatal menores caen bajo la prohibición del articulo 2(4) de la Carta ONU, independientemente de si califican como actos de agresión, o como ataques armados y facultan en consecuencia al Estado lesionado a recurrir a la autodefensa[23].

En Actividades Militares en Congo, sostuvo la CIJ que el artículo 51 de la Carta ONU justifica el ejercicio del derecho de autodefensa, aunque no debe ser utilizado a fin de proteger otros intereses, incluso los relativos a la seguridad del Estado. Por esto, consideró que Uganda había violado las obligaciones de abstención del uso de la fuerza y no intervención, ya que sus operaciones militares tenían por objeto asegurar ciudades y puertos, y apoyar la actividad de ciertos grupos en la guerra civil[24].

La cuestión de si un ciberataque es asimilable a un típico daño comercial frente al cual estaría habilitada la toma de contramedidas antes que un ataque armado, encuentra opiniones divididas. Quienes optan por considerarlo un daño producto de un hecho internacionalmente ilícito reparan mayormente en la naturaleza de la acción (degradar, detener, hackear un servicio de redes de computación) y explican que serían de aplicación las normas contenidas en el Proyecto de Artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos [25]. Quienes lo asimilan al uso

22 Ver Ian Brownlie, International Law and the Use of Force by States, (1963), pp. 362; 431.

23 CIJ, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), fondo, (1986), para. 191 y 195; *International law Commission, Report of the International Law Commission on the work of its Thirty-second session*, (05/05–25/07 1980), *Official Records of the General Assembly, Thirty-fifth session, Supplement No. 10, UN document* A/35/10, (1980), p. 44; Yoram Dinstein, War, *Aggression and Self-Defence, 4th ed.*, (2005), *p. 174 y ss.; Ian Brownlie, International Law and the Use of Force by States,* (1963), pp. 363-366.

24 CIJ, Actividades Armadas en el Territorio del Congo (República Democrática del Congo v. Uganda). Sentencia, (19/12/2005).

25 Comisión de Derecho Internacional, Proyecto de artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos, señalados a la atención de los gobiernos por la Asamblea General en la Resolución A/56/83 de 28/01/2002 (disponible en http://portal.uned.es/pls/portal/PORTAL.wwsbr_imt_services.GenericView?p_docname=22634788.PDF&p_type=DOC&p_viewservice=VAHWSTH&p_searchstring=, en 14/08/2018).

de la fuerza armada, consideran los efectos del ciberataque, que pueden consistir en la privación de derechos humanos básicos como ya se ha mencionado.

En suma, se encuentran distintos niveles de ilicitud:

- Primero, si una ciberoperación viola obligaciones impuestas al Estado por el DI general, genera responsabilidad internacional del Estado infractor.
- Segundo, si la ciberoperación constituye un ciberataque cuyas consecuencias son asimilables a las del uso de armamento cinético, químico, biológico o nuclear, debe entenderse enmarcada en la prohibición general del no uso de la fuerza conforme el artículo 2(4) de la Carta ONU [26].
- Tercero, queda por resolver si toda amenaza o uso de la fuerza constituye un ataque armado que habilita la autodefensa.

2. En caso que un ciberataque constituya un ataque armado, ¿puede utilizarse la legítima defensa conforme el artículo 51 de la Carta ONU?

Frente a un daño ocasionado por un Estado a otro, el Estado afectado puede conforme el DI general recurrir a dos tipos de medidas coercitivas: (I) las contramedidas y (II) la legítima defensa. Las primeras se entienden como un conjunto de acciones y omisiones tendientes a restaurar el respeto del DI e inducir al Estado infractor a cumplir las obligaciones derivadas de su responsabilidad por el ilícito cometido, sin recurrir al uso de la fuerza armada. La legítima defensa, por su parte, presupone un ataque armado por parte de un Estado contra otro, o en la concepción anglosajona -más amplia-, la 'inminencia' [27] de un ataque armado. Brinda al Estado lesionado la posibilidad de ejercer la fuerza contra el Estado agresor.

Si el eje divisorio pasa por la ocurrencia de un ataque armado, la controversia surge respecto de su calificación. En este sentido, la Resolución 3314 que define la agresión, brinda elementos básicos aunque insuficientes. Actos tales como la inva-

26 Schmitt, Michael, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law*, vol. 37 (1999), p. 916.

27 Tal como recuerda Barboza, la inminencia que diera lugar a la necesidad de defensa propia debiera ser "urgente, abrumadora, que no dejara lugar a la elección de los medios ni tiempo a la deliberación". Barboza Julio, Derecho Internacional Público, Zavalía Editor, 1 de., Buenos Aires, p. 245, (1999).

sión del territorio de un Estado por otro; el bloqueo naval de las costas; el ataque a las fuerzas armadas o sus bienes (bases, naves mercantes o de guerra) en cualquier lugar que fuera, constituyen ataques armados. Sin embargo, otras situaciones como la prolongación de la presencia de una fuerza militar extranjera en territorio de otro, producto de un previo ataque armado; o el apoyo a mercenarios o grupos armados que actúan allende las fronteras, son cuestiones abiertas a controversia.

Conforme el DI general, la legítima defensa tiene como propósito proteger el orden jurídico, en el cual se equilibran los derechos del Estado atacante con los del Estado agredido. Ahí se permite que este decida las medidas necesarias para repeler un ataque armado, incluido el uso de la fuerza. La justificación se encuentra en la ilicitud inicial de la conducta del Estado infractor y la necesidad de evitar el daño que pueda resultar de esa conducta ilícita. El incidente del Caroline (1837) sirvió para elaborar el llamado "test del Caroline de la legítima defensa", donde se establecen los requisitos para su legalidad[28]. Así establece que la necesidad de defenderse debe ser "instantánea, abrumadora y no dejar tiempo para la elección de los medios ni momento para la deliberación". Desde aquel momento, se han formulado modalidades y principios que, junto con su codificación en la Carta ONU, rigen el ejercicio de la legítima defensa.

Dentro del DI consuetudinario, los principios de necesidad y proporcionalidad determinan los requisitos necesarios para ejercer la autodefensa. El principio de necesidad define los márgenes de la legítima defensa. Requiere la previa existencia de una conducta ilícita ligada con el uso de la fuerza y la necesidad objetiva de evitar un nuevo ataque armado o repelerlo (necesidad cualitativa). Cumplida esta condición previa, el principio requiere, además, que las medidas adoptadas sean necesarias temporal y cuantitativamente para que la acción defensiva sea legítima.

Desde una perspectiva temporal, la acción de autodefensa no puede llevarse a cabo legalmente antes que sea realmente necesaria a fin de repeler un ataque armado, ni tampoco cuando ya no sea necesaria para tal propósito (necesidad temporal). De hecho, el objetivo de la autodefensa es prevenir la materialización del daño potencialmente resultante de una amenaza. Debe dirigirse 'contra' un ataque inminente o en curso con el objetivo de prevenirlo, rechazarlo y/o limitarlo a sus mínimos efectos. El requisito de necesidad temporal se considera por algunos autores como un tercer

28 Ver Arend, Anthony C., International Law and the Preemptive Use of Military Force (2003), en internet https://www.cfr.org/content/publications/.../03spring_arend.pdf , disponible en 18/08/2018.

requisito al que denominan de 'inmediatez'. El principio de proporcionalidad exige que el tipo y el grado de la fuerza utilizada en defensa propia no superen lo que es realmente necesario para repeler el ataque armado en cuestión.

En cuanto al DI convencional, las diferencias respecto de la extensión del "derecho inmanente de legítima defensa individual o colectiva" evitaron que la AG ONU pudiera incluir alguna provisión sustantiva en las resoluciones que intentaron codificar la costumbre internacional relativa al uso de la fuerza.

La Declaración sobre Relaciones Amistosas entre Estados (1970) y la Definición de la Agresión (1974) no incluyen provisiones sobre la autodefensa. En la Declaración sobre el No uso de la Fuerza (1987) no pudo avanzarse más allá de afirmar que los "Estados tienen el derecho inmanente de legítima defensa individual o colectiva si ocurre un ataque armado, como lo estipula la Carta de Naciones Unidas" (Treves, 1987).

También el CS trató la legítima defensa, sin avanzar sobre la letra de la Carta ONU. La Resolución 1368 (2001) fue una de las respuestas del CS al atentado terrorista del 11 de septiembre. En ella el CS reconoce el derecho inmanente de legítima defensa individual o colectiva. No obstante, exhortar a los Estados a cooperar para sancionar a los responsables, no adoptó medidas bajo el Capítulo VII de la Carta, ni autorizó una intervención armada en los territorios sospechados de albergar a al-Qaeda, sus células y máximos líderes.

Conforme lo hasta ahora comentado, la autodefensa no estaría permitida si se presentara como respuesta a un daño causado solamente por operaciones cibernéticas hostiles. La respuesta varía si el derecho pretende ejercerse con miras a prevenir o repeler un ataque inminente o en curso, y solo en la medida necesaria para lograr el fin. Además, el daño a infligir por acción cibernética autodefensiva en el atacante, terceros Estados o individuos no implicados, siempre debe estar justificado por la gravedad del daño a evitar. La velocidad, imprevisibilidad y la naturaleza clandestina de la mayoría de los ciberataques obstaculizan gravemente la capacidad del Estado defensor de reaccionar a tiempo para detectar y prevenir o repeler un ataque que bien puede programarse para producir sus efectos nocivos meses después de la intrusión. En cuanto a la autodefensa cibernética, depende de sistemas automatizados que hacen una evaluación y verificación de la identidad del atacante a fin de iniciar la acción defensiva. Esta circunstancia hace extremadamente difícil cumplir con los requisitos de necesidad y proporcionalidad.

Estas características específicas de las operaciones cibernéticas, junto con el hecho que los ataques son ejecutados por actores subrogados no estatales y, a su vez dependen de series de operaciones a pequeña escala, han llevado al ciberespacio la aún latente discusión sobre la legalidad de la ciber-defensa preventiva[29].

Si se resume la doctrina de la CIJ, pueden afirmarse ciertos principios rectores: (I) el ataque militar que sirve como justificación de la autodefensa debe ser significativo; (II) debe ser atribuible al Estado contra el que luego se ejerce la acción; (III) el ejercicio de la autodefensa debe constituir una última ratio; (IV) debe utilizarse en forma defensiva; y (V) debe ser proporcional al daño sufrido. Como se ve, en comparación con las contramedidas, la habilitación de la legítima defensa es restrictiva, en tanto implica una excepción a la prohibición general del uso de la fuerza. Por esto, la CIJ exige un ataque armado significativo, que la autodefensa constituya una última ratio que sea necesaria y proporcional.

¿Constituyen las ciberoperaciones ataques armados?: diferencia entre uso de la fuerza y ataque armado

Dentro del sistema de las Naciones Unidas, los Estados miembros confieren al CS la responsabilidad principal del mantenimiento de la paz y la seguridad internacionales (Carta ONU, Artículo 24). Cuando el CS determina la existencia de una "amenaza a la paz y la seguridad internacionales", puede autorizar las medidas que sean necesarias para mantener o restaurar los bienes protegidos (Carta ONU, Capitulo VII).

El ámbito de aplicación del artículo 2(4) de la Carta ONU que prohíbe el uso de la fuerza "contra la integridad territorial o la independencia política de cualquier Estado o en cualquier otra forma incompatible con los Propósitos de Naciones Unidas" es mayor que el del artículo 51, que afirma la legítima defensa. Esto es así en la medida que el primero prohíbe no solo la fuerza armada, sino otros tipos de fuerza -no armada- o bien modos indirectos de su utilización. Además, el artículo 2(4) prohíbe no solo el uso presente de la fuerza, sino también la amenaza del uso mediato.

29 Ver Schmitt, Michael, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, en Columbia Journal of Transnational Law*, vol. 37, (1999), pp. 932–33; Eric Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defence, Stanford Journal of International Law,* vol. 38, (2002), pp. 221–24; y Marco Roscini, *World Wide Warfare—Jus ad bellum and the Use of Cyber Force, en Armin Bogdany y Rüdiger Wolfrum (eds), Max Planck Yearbook of United Nations Law,* vol. 14, (2010), pp. 120–23.

El concepto de "amenaza a la paz" comprende un alto grado de subjetividad convirtiéndose casi en una cuestión política, brindándole al CS amplia discrecionalidad. Como cuestión de derecho, la determinación de una amenaza a la paz no presupone la existencia de un hecho internacionalmente ilícito, ni una amenaza o uso de la fuerza, ni tampoco la ocurrencia de un ataque armado en el sentido de la Carta de la ONU. La relevancia práctica de calificar una ciberoperación como ataque armado ordenado, ejecutado o auspiciado por un Estado, es que permitiría al Estado afectado decidir legalmente cualquier acción defensiva, incluido el uso de la fuerza.

No todo uso de la fuerza constituye un ataque armado. Algunos autores requieren que para que el uso de la fuerza califique como tal, debe ejecutarse en una escala relativamente amplia 30. Otros autores en cambio, dudan sobre la validez de este criterio basados en el principio de *minimis non curat lex* -la ley no se ocupa de asuntos menores-, y no ven la razón para excluir ataques ejecutados en pequeña escala de la categoría de ataque armado, en tanto sus consecuencias alcancen un piso mínimo de daños, tales como víctimas humanas o una seria destrucción de la propiedad del Estado atacado (Dinstein, Y., 2005, pp. 174–75)31. Jennings, Robert y Watts (1992) admiten que a pesar de la terminología utilizada por la CIJ, la línea divisoria entre un ataque armado y un mero incidente fronterizo es generalmente poco clara (p. 418), o bien simplemente equiparan la noción de ataque armado con el uso directo de la fuerza armada contra un Estado, con independencia de su escala o intensidad (Michael Schmitt, 1999, p. 929).

La noción de ataque armado implica necesariamente el uso de armamento. En la opinión consultiva sobre la legalidad de la amenaza o uso de armas nucleares, la CIJ aclaró que tanto el artículo 51 de la Carta ONU como los artículos 2(4) y 42 de igual documento, se aplican a "cualquier uso de la fuerza, independientemente del armamento empleado" (CIJ, 1996, p. 226, para. 39). Desafortunadamente, la CIJ no avanzó en explicar de manera específica y razonada no solo la distinción, sino las consecuencias

30 Randelzhofer, Albrecht, Article 51 UN Charter, en Bruno Simma (ed.), *The Charter of the United Nations: A Commentary,* vol. I, (2002), p. 796 (mencionando "relativamente a gran escala"); y Christopher Greenwood, *War, terrorism and international law, Current Legal Problems,* vol. 56, no. 1, (2003), p. 516 (mencionando "cierto nivel de gravedad) y p. 518 ("de suficiente intensidad").

31 Ver Dinstein, Yoram, War, Aggression and Self-Defence, 4th ed., (2005), pp. 174–75, y mas específicamente en relación con las ciberoperaciones, Yoram Dinstein, Computer Network Attacks and SelfDefense, en Michael Schmitt and Brian O'Donnell (eds), Computer Network Attack and International Law, (2002), p. 105.

jurídicas resultantes. Esto derivó en mayor confusión al momento de distinguir entre tipos graves y menos graves del uso de la fuerza, lo cual dificulta transpolar el concepto de ataque armado a una ciberoperación.

En tanto los ciberataques no utilizan el tradicional armamento cinético, biológico, químico o nuclear, su ejecución depende de un pre-requisito consistente en la infraestructura sobre la cual descansa el ciberespacio. Esto lleva a analizar los objetos que pueden ser considerados como arma. Al respecto, se ha afirmado que no es ni la designación del dispositivo, ni su uso normal lo que hace a la existencia de un arma, sino la intención con la que el objeto es utilizado y los efectos que genera. El uso de un dispositivo tecnológico o de un conjunto de ellos, del cual resulta una considerable pérdida de vidas o una destrucción extensiva de la propiedad del Estado lesionado debe considerarse condición suficiente para afirmar la existencia de un ataque armado (Zemanek, Karl, Armed attack, 2010, p. 21).

El término 'ataque' es un término técnico importante del DIH, ya que varias reglas sobre la conducción de las hostilidades se expresan a partir de tal concepto. Si se toman en consideración los Convenios de Ginebra y sus Protocolos Adicionales, se hallará a modo de ejemplo que no serán objeto de ataque (I) los establecimientos sanitarios (artículo 19, CI); (II) las aeronaves sanitarias, exclusivamente utilizadas para la evacuación de los heridos y de los enfermos, así como para el transporte del personal y del material sanitarios (artículo 36, CI y CII); (III) en ninguna circunstancia, los hospitales civiles (artículo 18, CIV); (IV) ninguna persona [fuera de combate] (artículo 41 PAI); (V) la población civil (artículo 13(2) PAII), entre otras menciones.

De especial interés es el artículo 49 del Protocolo Adicional I que afirma que se entiende por ataque los actos de violencia contra el adversario, sean ofensivos o defensivos (artículo 49 PAI). La definición desencadenó una discusión significativa relativa a la medida en que una ciberoperación -en vista de su naturaleza no cinética- podría considerarse un "acto de violencia" y por lo tanto, un "ataque" conforme el DIH.[32] Como ya mencionamos, es hoy generalmente reconocido que los actos de violencia no requieren necesariamente el uso de fuerza cinética, siendo suficiente que los efectos equivalgan a los que normalmente se asocian con ella, es decir, la muerte

32 Un ataque cinético se vale de la energía cinética que todo cuerpo posee debido a su movimiento. La energía se produce mediante la aceleración. Un antecedente de arma cinética fue la catapulta.

o lesión de personas o destrucción física de objetos[33]. Esta interpretación reconoce que las ciberoperaciones que desencadenan procesos que causen tales consecuencias constituyen verdaderos "actos de violencia" conforme el sentido establecido en el artículo 49 (1) PAI [34].

Un concepto de especial interés es el de la infraestructura crítica. Esta es una preocupación vital de los Estados al discutir cuestiones de ciberseguridad[35]. La Unión Europea menciona que la infraestructura crítica incluye:

> aquellos recursos físicos, servicios y recursos de tecnología de la información, redes y activos de infraestructura que, si se perturbaran o destruyeran, tendrían un impacto grave en la salud, la seguridad, el bienestar económico de los ciudadanos o el funcionamiento eficaz de los gobiernos.[36] .

Si se analiza el carácter disruptivo antes que destructivo de la mayoría de los ciberoperaciones, incluso la propuesta que repara en las consecuencias del ciberataque,

33 Dinstein, Yoram, Computer Network Attacks and Self-Defense, en Michael Schmitt and Brian O'Donnell (eds), Computer Network Attack and International Law, (2002), p. 103; Michael Schmitt, Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, vol. 84, no. 846, (2002), p. 373; Michael Schmitt, Cyber Operations and the Jus in Bello: Key Issues, Naval War College International Law Studies, (2011), pp. 6–7; Knut Dörmann, The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint, in Karin Byström (ed.), International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November (2004), Stockholm, Sweden, Swedish National Defence College, (2004).

34 Ver al respecto, la discusión sobre la participación directa en las hostilidades en relación con las operaciones colectivas y medidas preparatorias en Melzer, Nils, Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL, ICRC (2009), pp. 54–55, 65–67.

35 Ver por ejemplo, la Resolución AG ONU 58/199 de 30/01/2004 (Creación de una cultura global de ciberseguridad y la protección de infraestructuras de información críticas); La Directiva de Decisión Presidencial de EEUU 63, relativa a la "Protección de Infraestructura Crítica", de 22/05/1998; la Casa Blanca, "Estrategia Nacional de Protección Física e Infraestructura Crítica y Activos Principales" de 2003; y Comisión Europea, "Libro Verde del Programa Europeo sobre la Protección de la Infraestructura Crítica", documento COM(2005) 576 final, 17/11/2005. Ver igualmente Eric Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence", Stanford Journal of International Law, vol. 38, (2002), pp. 207 ss; Lesley Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", Loyola of Los Angeles International and Comparative Law Review, vol. 32 (2010), p. 306.

36 Ver documento citado en el punto anterior. "Critical Information Infrastructure (CII): ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)" .

es insuficiente para permitir la autodefensa. Por esta razón, cobra impulso el criterio de la "escala y efectos" del ataque que descansa en el daño a la 'infraestructura crítica' del Estado y la equipara casi por completo a la destrucción física de personas o cosas. Si se utiliza este criterio puede argumentarse que todo ciberataque del cual no resultara la muerte, daños o destrucción a personas o cosas, calificaría aún como ataque armado si su propósito fuera incapacitar la 'infraestructura crítica' dentro de la esfera de soberanía de otro Estado.

Primero, no toda amenaza o uso de la fuerza prohibidos por el articulo 2(4) de la Carta ONU constituyen automáticamente un ataque armado que justifique una acción de autodefensa[37]. Segundo, conforme la interpretación de la CIJ, solo las formas más graves del uso de la fuerza califican como ataque. Tercero, el uso de armamento es una condición esencial para la existencia de un ataque armado.

En suma, las ciber-operaciones pueden calificar como ataque armado en la medida que los actos de violencia sean graves y produzcan como consecuencia la muerte o lesiones de personas o destrucción de bienes. En este punto, los daños a la infraestructura crítica de los Estados se interpretan como 'destrucción' aun cuando no se exprese físicamente. Finalmente, todo objeto cibernético del cual resulte la muerte, lesión o destrucción puede ser considerada como un arma.

3. ¿Es posible aplicar las reglas y principios del Derecho Internacional Humanitario a un ciberconflicto?

El DIH se propone "humanizar la guerra" (Kalshoven, F., y Zegveld, L., 2003, p. 12). En sus dos vertientes de la Haya y de Ginebra, se dirige a los Estados, tanto para limitar sus formas de interacción en el conflicto armado, como para imponerles obligaciones

37 Ver Randelzhofer, Albrecht, Article 51 UN Charter, en Bruno Simma (ed.), The Charter of the United Nations: A Commentary, vol. I, (2002), p. 790. De igual manera, Yoram Dinstein, War, Aggression and Self-Defence, 4th ed., (2005), pp. 167, 174; Ian Brownlie, International Law and the Use of Force by States, (1963), p. 278 y ss.. La existencia de esta brecha fue confirmada por el DI consuetudinario en CIJ, Actividades Militares y Paramilitares en y contra Nicaragua (Nicaragua v. United States of America), fondo, (1986), para. 191, donde la CIJ consideró que era "necesario distinguir las formas mas graves de uso de la fuerza (aquellas que constituyen un ataque armado) de otras menos graves" (confirmado luego en CIJ, caso de las Plataformas Petroleras, Irán v. Estados Unidos, 06/11/2003).

respecto de las personas que sufren las consecuencias[38]. Surgen así dos principios fundantes: (I) "el derecho de las Partes en conflicto a elegir los métodos o los medios de guerra no es ilimitado" (La Haya); y (II) "las personas puestas fuera de combate y las que no participan directamente en las hostilidades serán respetadas, protegidas y tratadas con humanidad" (Ginebra)[39].

El objeto básico del DIH consiste en la "ayuda desinteresada para todas las víctimas de la guerra sin discriminación, para todos aquellos que (…) ya no son más enemigos sino solamente sufrientes e indefensas personas humanas" (International Committee of the Red Cross, 1949, p. 1). La protección se proporciona no contra la violencia de la guerra en sí, sino "contra el poder arbitrario que una parte obtiene, en el transcurso de un conflicto armado, sobre las personas que pertenecen a la otra parte" (Kalshoven, Frits y Zegveld, Liesbeth, 2003, p. 59). En cuanto a los principios de la acción humanitaria [40], la "Cláusula Martens" resume la aspiración primera del DIH:

> Mientras que se forma un Código más completo de las leyes de la guerra, las Altas Partes Contratantes juzgan oportuno declarar que, en los casos no comprendidos en las disposiciones reglamentarias adoptadas por ellas, las poblaciones y los beligerantes permanecen bajo la garantía y el régimen de los principios del Derecho de Gentes

38 El derecho de La Haya y de Ginebra, respectivamente. Ver Bugnion, François. El derecho de Ginebra y el derecho de La Haya, Revista Internacional de la Cruz Roja, 31/12/2001, N° 844. pp. 901 – 922. Respecto del Derecho de La Haya, ver Hensel, Howard M., The law of armed conflict: constraints on the contemporary use of military force, Aldershot, Hants, England; Burlington, VT : Ashgate Pub. Co., (2005); Human rights watch Medio Oriente: proyecto Armas, Civilian pawns: laws of war violations and the use of weapons on the Israel-Lebanon border New York: Human Rights Watch, (1996). En relación al Derecho de Ginebra, ver Valencia Villa, Alejandro, La humanización de la guerra: derecho internacional humanitario y conflicto armado en Colombia, Bogotá, Colombia: Ediciones Uniandes: Tercer Mundo Editores, (1991); Reglas básicas de las Convenciones de Ginebra y sus protocolos adicionales, CICR, Ginebra, (1983); Bory, Francoise, Origen y desarrollo del derecho internacional humanitario, CICR, (1982).

39 Pictet, Jean, Desarrollo y Principios del Derecho Internacional Humanitario, Curso del Instituto de Derechos Humanos de Estrasburgo, Universidad Robert Schuman, 1982, p. 31.

40 Pictet, Jean, Development and principles of international humanitarian law, Dordrecht, Neth: Martinus Nijhoff Publishers, (1985).

preconizados por los usos establecidos entre las naciones civilizadas, por las leyes de la humanidad y por las exigencias de la conciencia pública.[41].

La CIJ (1996) en su Opinión Consultiva sobre la legalidad del uso de armas nucleares, invocó la Cláusula Martens al afirmar la vigencia de los principios y reglas del derecho humanitario y aplicarlos a la amenaza y uso de las armas nucleares.

El DIH se basa "en el principio fundamental que las personas protegidas deben ser respetadas (obligación pasiva) y protegidas (obligación activa) en todas las circunstancias y recibir un trato humano sin distinción alguna de índole desfavorable basada en el sexo, raza, nacionalidad, religión, opiniones políticas o en cualquier otro criterio análogo" [42]. Conforme el principio de no discriminación: "Las personas serán tratadas sin distinción alguna fundada en la raza, el sexo, la nacionalidad, el idioma, la clase social, la fortuna, las opiniones políticas, filosóficas o religiosas, o en otro criterio análogo".[43]

Al preguntarse por la posibilidad de aplicar el DIH a los ciberconflictos, se enfrentan al menos dos escenarios distintos. Primero, el ciberataque puede ejecutarse en el contexto de un conflicto armado convencional. Segundo, la ciberoperación puede existir en forma aislada y orientarse a degradar o dañar personas, bienes o infraestructura crítica del Estado atacado. Dentro de este segundo supuesto, cabe distinguir entre aquellos que producen daños concretos en el mundo físico y aquellos que no se manifiestan de manera visible [44]. En relación con el primer supuesto, no es la naturaleza precisa de un medio o método, sino el contexto en el que los mismos son utilizados, lo que somete una conducta a las reglas y los principios del DIH. Por lo

41 La Cláusula Martens aparece por vez primera en el Preámbulo del (II) Convenio de La Haya de 1899 relativo a las leyes y costumbres de la guerra terrestre. La Cláusula es introducida por el Delegado Ruso, profesor von Martens en la Conferencia de la Paz de La Haya de 1899. Ver Fiódor Fiódorovich Martens (1845-1909) -humanista de los tiempos modernos, Revista Internacional de la Cruz Roja (RICR), no 135, mayo-junio de 1996, pp. 324-339. Ver Kalshoven, V. F., Constraints on the Waging of War, Martinus Nijhoff, Dordrecht, 1987, p. 14.

42 CG I y II, Artículo 12; CG III, Artículo 16; CG IV, Artículo 27. Ver Kalshoven Frits y Zegveld Liesbeth, op. cit., p. 62.

43 Artículo 3 común a los cuatro Convenios de Ginebra, III Convenio de Ginebra 12/08/1949, Comentario del artículo bajo la dirección de Jean Pictet. Fórmulas de la misma índole fueron introducidas en varias disposiciones de los Protocolos de 1977, especialmente en el preámbulo y en los artículos 10 y 75 del Protocolo I, así como en el artículo 2 del Protocolo II.

44 Por ejemplo, ciberoperaciones que ralentizan una intranet comercial o militar, descargan información financiera o personal, hacen perder temporalmente el acceso a Internet o a sitios web, o practican el ciberespionaje.

tanto, lejos de importar si la ciberoperación que ocurre en el contexto de un conflicto armado ya existente, parte del territorio de uno de los Estados beligerantes, lo que resulta decisivo es si tal ataque se encuentra relacionado con el conflicto en curso. En palabras del Tribunal Penal Internacional para la ex Yugoslavia (TPIY), es imprescindible la existencia de un nexo con uno de los grupos armados del conflicto. De ser así, es evidente que las reglas del DIH se aplican a los eventuales ciberataques. Respecto del supuesto relativo a una ciberoperación no relacionada con un conflicto armado convencional, la respuesta es menos concluyente. Tradicionalmente, según Beard, Jack (2014) los Estados han reservado la aplicación del DIH para actos de violencia física directa, donde se excluyen los daños producidos por conductas que no constituyen violencia física.

El Manual de Tallin afirma la distinción entre conflictos armados internacionales y no internacionales, y reconoce que las ciber-operaciones pueden por sí mismas constituir un ataque armado, dependiendo de las circunstancias y especialmente, de sus efectos destructivos. El Manual define un ciberataque como "una operación cibernética, ya sea ofensiva o defensiva, que razonablemente se espera que cause lesiones o muerte a personas o daños o destrucción de objetos".

La cuestión básica consiste en calificar como 'daño' en el mundo digital. La mayoría de los expertos que redactaron el Manual acordaron que además del daño físico, la pérdida de funcionalidad de un objeto también constituye un daño. El Comité Internacional de la Cruz Roja entiende que es irrelevante la manera en que un objeto es desactivado, sea por medios cinéticos o por una ciberoperación. Este punto es esencial, ya que, de lo contrario, una operación cibernética destinada a distorsionar una red civil no estaría cubierta por la prohibición humanitaria de no atacar directamente personas y objetos civiles.

El caso de las plataformas petroleras ofrece comentarios útiles a fin de determinar si un ataque no convencional -como es un ciberataque-, puede por sí solo, alcanzar el nivel de ataque armado. La CIJ (2003) destacó que:

> la cuestión es "si tal ataque, considerado en sí mismo o en combinación con el resto de las 'series de (…) ataques' citados por los Estados Unidos puede ser categorizado como un ataque armado que justifique la autodefensa de Estados Unidos.

Este análisis acumulativo de la CIJ dio lugar a la llamada doctrina de la acumulación, por la cual, de sumarse una serie de acontecimientos sin solución de continuidad, se podría estar en presencia de un ataque armado. Así, ciberoperaciones que en sí mismas no poseían tal carácter, podrían obtenerlo a partir de su sumatoria aislada o en combinación con otros acontecimientos. Por ejemplo, microataques de hackers individuales que combinados constituyen un ataque masivo.

Conclusiones

Si bien no han existido hasta el momento consecuencias humanitarias dramáticas producidas por ciberataques, la creciente dependencia de los sistemas controlados por computadora para sostener las vidas diarias implica un riesgo a futuro cada vez mayor. Hasta la fecha solo se ha experimentado una pequeña fracción de las posibilidades de conflicto cibernético, y la experiencia real ha sido limitada. De hecho, casi todas las acciones adversas que se sabe que se tomaron en el ciberespacio contra los Estados Unidos o cualquier otra nación, incluidos el ataque cibernético, no alcanzaron el umbral para calificarlas como "uso de fuerza o ataque armado".

La principal característica de Internet es su anarquía estructural. No existen distinciones funcionales entre redes militares o civiles ni entre jurisdicciones estatales. En potencia todo está conectado a todo. El futuro inmediato solo puede aspirar a profundizar la tendencia: se afirma que evolucionará hacia una mayor incertidumbre con el almacenamiento de datos y contenidos en la nube. Con el uso de la computación en la nube, existen escenarios viables donde los datos de grupos terroristas o beligerantes se almacenan en la misma nube uno al lado del otro, sin que las partes lo sepan.

La transposición de reglas y principios desarrollados por el DI general, tanto consuetudinario como convencional a lo largo de su historia, capta parcialmente el fenómeno de las NTIC empleadas como armas para realizar operaciones ofensivas y defensivas entre Estados y entre estos y otros actores del sistema internacional. A partir de esta captación parcial se plantean una serie de interrogantes: algunos pueden resolverse al aplicar las fuentes tradicionales del DI general, aunque en la mayoría de los casos, las respuestas poseen matices propios.

De las cuestiones relevantes en cuanto a las consecuencias dañosas de los ciberataques, en este artículo hubo un interés por: (I) caracterizar un ciberataque y conocer

bajo qué circunstancias puede constituir un ataque armado; (II) la posibilidad de utilizar la autodefensa por parte del Estado afectado; y (III) las normas de DI aplicables a los ciberataques y los desafíos que plantea la aplicación del DIH a este nuevo tipo de armamento.

Si se tienen en cuenta las restricciones legales, la realización de ataques cibernéticos es difícil y desafiante, pero es posible. La pregunta permanece: ¿es la ley actual suficiente para abordar los ciberataques? A pesar que el DIH no pudo prever los ciberataques en su inicio, sus principios y normas fundamentales son suficientemente flexibles. No obstante, la ausencia de normas internacionales consuetudinarias es una preocupación en este campo, y brinda libertad a los Estados para actuar conforme sus intereses, modelando así la futura costumbre internacional.

Referencias

Abi-Saab G., (1989). *The Concept of "International Crimes" and its Place in Contemporary International Law*, en J. Weiler, M. Spinedi, y A. Cassese (eds.), International Crimes of State: a Critical Analysis of the ILC's Draft Article 19 on State Responsibility, W. de Gruyter, Berlin/ New York.

Artiles, Néstor. *La Situación de la ciberseguridad en el ámbito internacional y en la OTAN. Instituto Español de Estudios Estratégicos (IEEE)*. Cuaderno de Estrategia N° 149.

Bodansky Daniel y Crook John R., (1963). *Symposium: The ILC's State responsibility articles introduction and overview, The American Journal of International Law*, Vol. 96.

Brownlie Ian. (1963). *International Law and the use of Force by States.* Oxford University Press.

C. Pilloud y J. Pictet. (1987). *Article 49. Definition of Attacks and Scope of Application*. L Y. Sandoz et al. (eds). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Geneva: Martinus Nijhoff, pp. 601L608.

Cano, Jeimy. (2011). *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global.* N° 119 (abr-Jun. 2011) Revista Sistemas, Colombia.

Combacau Jean y Sur Serge. (2016). Droit International Public, 12 edición, LGDJ, Lextenso, Issy les Moulineaux, Francia.

Crawford J., Pellet A., and Olleson S. (2010). *The Law of International Responsibility*. Oxford University Press.

Crawford, James. (2002). *(comp). The International Law Commission's articles on State Responsibility.* Cambridge University Press.

CIJ. (1996). *Legality of the Threat or Use of Nuclear Weapons, advisory opinion,* p. 47.

Derby, Daniel, H. *A framework for International Criminal Law, in International Criminal Law*, Bassiouni, M. Cherif (ed.), Vol. 1 Crimes.

Dörmann, K., (2004). *Applicability of the Additional Protocols to Computer Network Attacks. L ICRC*. Conduct of Hostilities, Information Warfare.

Dinstein, Y. Computer Network Attacks and Self-Defense. Computer Network Attack and International Law 99.

International Committee of the Red Cross. (1949). *The Geneva Conventions of August 12*. Geneva, Preliminary Remarks.

Journal Transnational Law 67. (2014). *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law*, 47 Vand.

Kaczorowska, Alina. (2005). *Public International Law*. 3rd edition, Old Bailey Press, London.

Kalshoven, Frits y Zegveld, Liesbeth. (2003). *Restricciones en la conducción de la Guerra, Introducción al derecho internacional humanitario*. CICR, Buenos Aires.

Kodar, E., (2012).*Applying the Law of Armed Conflict to Cyberattacks: from the Martens Clause to Additional Protocol I, en Estonian National Defence College (ENDC) Proceedings*, Volume 15.

Lin, Herbert. (2012). , Cyber conflict and international humanitarian law. , *en International review of the Red Cross*, Volume 94 Number 886 Summer.

Malanczuk, Peter, Akehurst's. (1997). *Modern Introduction to International Law.* , 7th revised ed. Routledge, London, UK.

Michael N. Schmitt y Brian T. O'Donnell (2002). *US Naval War College International Law Studies*. Vol. 76.

Michael S., (1999). *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*. Columbia Journal of Transnational Law, vol. 37.

Morozov, E., (2008). *An Army of Ones and Zeroes: How I Became a Soldier in the Georgian-Russian Cyberwar*. L Slate.com.

NATO Cooperative Cyber Defence Centre of Excellence, Tallin, Estonia. En internet https://ccdcoe.org/index.html disponible a agosto 2018.

Nino, Carlos S., (1996). *El Castigo como Respuesta a las Violaciones a los Derechos Humanos: Una Perspectiva Global*, Título original: "Punishment as a Response to Human Rights Violations". P, publicado en Radical Evil on Trial, Carlos Santiago Nino, Yale University Press, New Haven y Londres.

Ottis, R., (2009). *On Definitions. L Conflicts in Cyberspace.*

Schmitt, M., (2002). Wired Warfare: Computer Network Attack and Jus In Bello. L *International Review of the Red Cross*, Vol. 84, No. 846.

Treves, T., (1987). *La Declaration des Nations Unies sur le renforcemente de l'efficacité du principe du non recours a la force.* Annuaire Français de Droit International.

Watts, S., (2010). *Combatant Status and Computer Network Attack. L Virginia Journal of International Law*, Vol. 50.

Waxman, Matthew, (2011). *Cyber Attacks as "Force" under UN Charter Article 2(4), Columbia Law School Scholarship Archive.*

AREANDINA

Fundación Universitaria del Área Andina