Ius Humani
Revista de Derecho. Vol. 9 (II) (2020), pp. 389-420. ISSN: 1390-440X — eISSN: 1390-7794
Recepción: 26-6-2020. Aceptación: 18-9-2020. Publicación electrónica: 10-12-2020
https://doi.org/10.31207/ih.v9i2.250

COVID-19 2.0. DERECHO INTERNACIONAL Y PROTECCIÓN DEL DERECHO A LA SALUD EN EL CIBERESPACIO: UNA VISIÓN DESDE ECUADOR

COVID-19 2.0. INTERNATIONAL LAW AND THE PROTECTION OF THE RIGHT TO HEALTH IN CYBERSPACE: A PERSPECTIVE FROM ECUADOR

Martín Roberto Tamayo Serrano [*]
Víctor Pacaric Calderón Merino[**]

Resumen: El objetivo de este artículo es explorar la oportunidad que presenta la crisis del Covid-19 en Ecuador para interpretar el Derecho internacional de los derechos humanos y el Derecho internacional humanitario de manera favorable a proteger el derecho a la salud y los sistemas de asistencia salud en el ciberespacio. A través de una metodología descriptiva que permite un análisis integral de la temática desde el punto de vista jurídico, el artículo sintetiza los principales debates internacionales sobre el alcance de la protección del derecho a la salud al amparo del Derecho internacional de los derechos humanos frente a amenazas cibernéticas; estudia la protección que brinda el Derecho internacional humanitario a los ciudadanos y a los sistemas de asistencia de salud; y

[*] Máster en Derecho (LL.M.) con mención en Derecho internacional público por London School of Economics and Political Science (Reino Unido). Especialista Superior en Derechos Humanos por la Universidad Andina Simón Bolívar (Quito, Ecuador). Abogado por la Universidad San Francisco de Quito (Ecuador). Analista en el Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador. https://orcid.org/0000-0002-4335-4293. martintamayo1@gmail.com

[**] Magíster en Relaciones Internacionales con mención en seguridad y derechos humanos por FLACSO (Quito, Ecuador). Diplomado de Postítulo en Transparencia, Accountability y Lucha contra la Corrupción por la Universidad de Chile (Santiago de Chile). Licenciado en Derecho por la Universidad de Salamanca (España). Experto 2 en el Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador. https://orcid.org/0000-0003-2876-3483. victor.pcm@hotmail.com

examina la situación del Ecuador, como un país que se enfrenta a varios retos en la aplicación de las políticas para asegurar la protección del derecho a la salud y los sistemas de asistencia de salud. El artículo concluye que los desarrollos normativos en ambos sectores no han logrado establecer una protección aceptada y efectiva, con obligaciones claras para los Estados en el espacio cibernético para proteger a las personas y a los sistemas de asistencia de salud. Asimismo, señala que las lagunas del Derecho internacional respecto a la protección de la salud en el ciberespacio se agravan en Ecuador al producirse una disonancia discursiva entre política exterior y nacional, con un impacto en la protección del derecho a la salud.

Palabras clave: Ciberseguridad, Covid-19, derechos humanos, derecho internacional, cuidado de la salud

---

Abstract: *The purpose of this article is to explore the opportunity offered by the Covid-19 crisis in Ecuador to interpret international human rights law and international humanitarian law to protect the right to health, and also health-care systems in cyberspace. Through a descriptive methodology that allows a comprehensive analysis of the issue from a legal point of view, this article: synthesizes the main international debates on the scope of the protection of the right to health under the international human rights law against cyber threats; studies the protection that international humanitarian law provides to citizens and health-care systems; and examines Ecuador's situation, as a country facing several challenges in the application of the necessary policies to ensure the protection of the right to health and health-care systems. The article concludes that the legal developments in both sectors have not managed to establish means of protection which are acceptable and effective, with clear obligations for States in cyberspace to protect individuals and health-care systems. Additionally, it argues that the gaps in international law regarding the protection of health in cyberspace are exacerbated in Ecuador by a discursive dissonance between foreign and domestic policy, with an impact on the protection of the right to health.*

Keywords: *Cybersecurity, Covid-19, Human Rights, International Law, Health Care*

Summary. *I. Introducción. II. Notas conceptuales sobre DI humanitario y DI-DDHH en relación con la protección de la salud en el ciberespacio. III. DI-DDHH y protección del derecho a la salud en el ciberespacio. III.1. Alcance de las obligaciones de los Estados al amparo del Derecho internacional de los derechos humanos. III.2. Aplicación general del Derecho internacional al ciberespacio,*

incluido el DI-DDHH en la protección del derecho a la salud. IV. Desafíos del DI humanitario en la protección de los sistemas de asistencia de salud en el ciberespacio. V. Disonancia discursiva en la política exterior ecuatoriana sobre la protección del derecho a la salud en el ciberespacio. VI. Consideraciones finales. Referencias.

I. INTRODUCCIÓN[1]

Desde el inicio de la declaración mundial de la pandemia por Covid-19 en febrero de 2020, se multiplicaron de manera inquietante los ciberataques dirigidos contra la infraestructura hospitalaria de varios países (República Checa, Reino Unido y Estados Unidos), y contra las instalaciones cibernéticas pertenecientes a la Organización Mundial de la Salud (Mačák *et al.*, 2020), entre otros.

La preocupación frente a estas situaciones reavivó los debates internacionales sobre la fortaleza del derecho internacional de los derechos humanos (DI-DDHH) y del derecho internacional humanitario (DI humanitario) en la protección del derecho a la salud y de los sistemas de asistencia de salud en el ciberespacio. La inquietud se mantuvo aún varios meses después, pues según varios expertos, en septiembre de 2020, tuvo lugar la primera muerte conocida de un paciente en un hospital que haya sido provocada directamente por un ciberataque (Howell, 2020).

En las condiciones de vulnerabilidad actuales —derivadas de la pandemia global por Covid-19— es pertinente explorar el contorno normativo de la aplicación del DI-DDHH y del DI humanitario, respectivamente, para fortalecer la protección cibernética del derecho a la salud y, consiguientemente, de los sistemas de asistencia de salud. Este análisis adquiere aún más relevancia, pues el impulso humanitario del Derecho internacional, especialmente en las dos ramas mencionadas, permite diagnosticar la manera en que las crisis revelan los límites y oportunidades de las normas orientadas a mitigar el sufrimiento humano en condiciones extremas (Sarat & Lezaun, 2009, pp. 10-19).

Bajo esta óptica, el presente artículo reflexiona acerca de los retos en la construcción y aplicación del DI-DDHH y DI humanitario aplicable a operaciones cibernéticas con relación al derecho a la salud y a los sistemas de asistencia de salud en un país que vivió una crisis nacional que obligó, como en otros, a emitir una declaratoria de emergencia sanitaria y un estado

[1] Si bien los autores mantienen un vínculo laboral con el Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador, las manifestaciones aquí efectuadas son personales y en ningún caso reflejan una posición institucional del Ministerio o del Gobierno ecuatoriano.

de excepción (Presidencia de la República de Ecuador, 2020; Zibel, 2019). En este sentido, el objetivo del artículo es explorar la oportunidad que presenta esta crisis en Ecuador para interpretar el DI-DDHH y el DI humanitario de manera favorable a proteger el derecho a la salud y los sistemas de asistencia salud en el ciberespacio, a la luz de los debates inter-estatales sobre la materia.

Para ello, y a fin de ponderar adecuadamente —desde un punto de vista jurídico— el impacto del Covid-19 en Ecuador (Zibel, 2020), cabe preguntarse estructuradamente sobre el grado de aplicabilidad del DI-DDHH y el DI humanitario, en lo que se refiere a las *zonas grises* del Derecho internacional en el ciberespacio identificadas por Michael Schmitt (Schmitt, 2017a, p. 17), como una manera de fortalecer la protección de las facilidades sanitarias y el derecho a la salud.

Para enriquecer el análisis jurídico que se deriva de esta problemática, el presente artículo se estructura en tres apartados. En primer lugar, se sintetizan los principales debates internacionales sobre el alcance de la protección del derecho a la salud al amparo del DI-DDHH frente a amenazas cibernéticas. Para ello, se analizan los estándares establecidos en los sistemas interamericano y universal, incluido su nivel de recepción en el Ecuador a través de análisis jurisprudencia, estudios doctrinales y de actores de la sociedad civil, así como el posicionamiento público de los Estados con relación a las obligaciones de Derecho internacional.

En segundo lugar, se estudia la protección que brinda el DI humanitario a los ciudadanos y a los sistemas de asistencia de salud. El estudio se enfoca en la posición de los organismos internacionales con componentes deliberativos intergubernamentales como el Comité Internacional de la Cruz Roja (CICR) y Naciones Unidas, la de los Estados, así como los aportes doctrinales. En estos espacios, se proponen interpretaciones consistentes con la necesidad de fortalecer la protección de los sistemas de asistencia de salud, así como soluciones alternativas respecto a la indefinición de la aplicación del DI humanitario en el espacio cibernético.

En tercer lugar, el artículo examina la situación concreta del Ecuador, como un país que mantiene internacionalmente una determinada posición en materia de derechos humanos, DI humanitario y ciberseguridad, pero que se enfrenta a varios retos en la aplicación nacional de las políticas necesarias para asegurar la protección del derecho a la salud y los sistemas de asistencia de salud.

II. NOTAS CONCEPTUALES SOBRE DI HUMANITARIO Y DI-DDHH EN RELACIÓN CON LA PROTECCIÓN DE LA SALUD EN EL CIBERESPACIO

En este estudio se adopta una perspectiva de investigación descriptiva desde el punto de vista metodológico. Según Cerda (2002), este tipo de investigación busca «describir las partes, categorías o clases que componen un objeto de estudio, o en su defecto, describir las relaciones que se dan entre el objeto de estudio con otros objetos» (p. 74). Por ello, desde el punto de vista jurídico resulta necesario primeramente conceptualizar el derecho a la salud, así sea de manera instrumental para avanzar en la exposición.

Al respecto, a pesar de la existencia de una multitud de definiciones (de Currea-Lugo, 2005, p. 29), se puede afirmar que el derecho humano a la salud no significa que implique una facultad de poder exigir individualmente un «derecho a estar sano», sino que más bien conlleva la idea prestacional de accesibilidad (Müller, 2014, pp. 39-40). Ello, a su vez, implica un derecho a disfrutar de «un sistema de salud eficaz e integrado, que abarque la atención de la salud y los determinantes subyacentes de la salud, y que responda a las prioridades nacionales y locales y sea accesible para todos» (Hunt & Backman, 2008).

Concordantemente con esta definición, el marco legal del DI-DDHH ha desarrollado obligaciones a nivel global y regional sobre el contenido del derecho a la salud. En particular, destaca el art. 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC) sobre el derecho al más alto nivel posible de salud (Pacto Internacional de Derechos Económicos, Sociales y Culturales, 1976). Por ello, es relevante la Observación General No. 14 del Comité de Derechos Económicos, Sociales y Culturales (2000), que desarrolla el contenido de dicho artículo. Asimismo, el art. 10 sobre el derecho a la salud del Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales (Protocolo de San Salvador) también constituye un elemento que será analizado desde su amplitud normativa (Protocolo adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales "Protocolo de San Salvador", 1988).

Por su parte, la protección jurídica —desde el DI humanitario— de las facilidades y personal sanitarios, incluidos medios de transporte de heridos y de enfermos o de material sanitario, se deriva de la aplicación de los cuatro Convenios de Ginebra de 1949 sobre DI humanitario y sus tres Protocolos Adicionales. En este sentido, en el presente artículo, la expresión «sistemas de asistencia de salud» se circunscribe en general a las unidades o

instalaciones médicas u hospitalarias, incluyendo cualquier establecimiento, en su aspecto físico y digital, destinado a fines sanitarios, así como al personal médico, en el sentido enunciado en las definiciones del art. 8 del Protocolo Adicional I a los Convenios de Ginebra.

Esta referencia al DI humanitario no se efectúa como un todo indivisible, sino que se refiere en Ecuador, en particular, a los artículos 38 a 44, 53 y 54 del Convenio de Ginebra I (1950); los artículos 41 a 45 del Convenio de Ginebra II (1950); y los artículos 18 a 22 del Convenio de Ginebra IV (1950). Las unidades sanitarias deben ser «respetadas y protegidas en todo momento» (Protocolo adicional II a los Convenios de Ginebra de 1949, 1978) y no pueden ser objeto de ataques al gozar un estatus civil, conforme al art. 12 del Protocolo Adicional I a los Convenios de Ginebra. El art. 54 del mismo Protocolo I, basado en el principio de distinción, restringe los métodos o medios de guerra que no puedan ser dirigidos a un objetivo militar o cuyos efectos no puedan ser legalmente limitados sobre la población civil (Protocolo adicional I a los Convenios de Ginebra de 1949, 1978). Extensivamente, el CICR aboga por la aplicación del DI humanitario, incluido el principio de distinción, al ciberespacio, basándose en el art. 36 del Protocolo I respecto a nuevas armas desarrolladas en el futuro (Christory, 2019, p. 4).

En este contexto, la protección cibernética con relación al derecho a la salud se refiere al resguardo que se brinda sobre los referidos sistemas de asistencia de salud que se realiza través de medios informáticos, y particularmente a la integridad en la utilización de sistemas informáticos interconectados, con especial atención a la utilización de Internet. Una definición más refinada conceptualmente de la noción de seguridad cibernética vinculada con derechos humanos y paz corresponde a la construcción de una red de regímenes multiniveles que promuevan una ciberseguridad sostenible, aclarando las reglas de actuación para los países y ayudar a reducir las amenazas de ciberconflictos, el cibercrimen y el ciberespionaje a niveles comparables a otros riesgos cinéticos (Shackelford, 2017, p. 13).

III. DI-DDHH Y PROTECCIÓN DEL DERECHO A LA SALUD EN EL CIBERESPACIO

III.1. Alcance de las obligaciones de los Estados al amparo del Derecho internacional de los derechos humanos

Desde el punto de vista del Derecho internacional de los derechos humanos (DI-DDHH), el contenido del derecho a la salud puede articularse

a través de tres tipos de obligaciones fundamentales expuestas por el Comité de Naciones Unidas sobre Derechos Económicos, Sociales y Culturales: de *respetar* —asegurando de manera negativa que el Estado no interfiera en disfrute del derecho—, de *proteger* —asegurando que otros actores diferentes del Estado no interfieran en el disfrute del derecho—, y de *cumplir* —garantizando de manera positiva que el mismo pueda ser efectivamente disfrutado (Clapham, 2007, p. 129). Desde la posición de la Asamblea General de Naciones Unidas (2014), el derecho a la salud aplica en esas mismas condiciones en el plano cibernético.

Trasladando la referida tríada de obligaciones internacionales al ámbito de las obligaciones en el ciberespacio, se puede decir, en primer lugar, que el Estado está obligado a asegurar, por ejemplo, que sus Instituciones no limitan o deniegan atenciones, en el plano cibernético, el acceso a los servicios de salud, sean de carácter preventivo, curativo o paliativo (Clapham, 2007, p. 130). En segundo lugar, implica que el Estado debe, por ejemplo, adoptar normativa que permita asegurar, también en el plano cibernético, un acceso igual a los servicios de salud que proveen otros actores diferentes de los estatales, como pueden ser las empresas (Clapham, 2007, p. 130). Finalmente, supone adoptar una política nacional de salud con un plan para garantizar el acceso a la salud, tomando en consideración también el aspecto cibernético (Clapham, 2007, p. 131).

Por ejemplo, este marco general sobre el derecho a salud ha constituido una plataforma conceptual para trabajar en materia de ciberseguridad y derecho a la salud. Recientemente, en mayo de 2020, un grupo de académicos en Derecho internacional emitió la *Declaración de Oxford sobre la protección del Derecho internacional contra ciberoperaciones dirigidas contra el sector sanitario* (Okande *et al.*, 2020). Este pronunciamiento articula una lista de siete puntos de consenso sobre regulación mínima de las operaciones cibernéticas dirigidas contra personas y sistemas de asistencia de salud. En particular, se considera que los Estados deben respetar y garantizar el derecho a la vida y el derecho a la salud de todas las personas que se encuentran dentro de su jurisdicción, incluso mediante la adopción de medidas que impidan que terceros interfieran en esos derechos por medios cibernéticos (Okande *et al.*, 2020). Se constata de manera clara que la orientación técnica y el análisis en esta materia se dirige a proponer obligaciones y principios, como los de Declaración, que son analizados desde las perspectivas del Derecho internacional aplicable a ciberoperaciones, DI-DDHH y DI humanitario.

A su vez, a nivel normativo, los compromisos internacionales en derechos humanos podrían regular la conducta de los Estados en lo que se refiere a sus obligaciones de respetar, proteger y cumplir con el derecho a la

salud en el ciberespacio frente a la pandemia por Covid-19. Varios instrumentos internacionales han desarrollado el contenido del derecho humano a la salud como un bien público que obliga al Estado a generar condiciones para asegurar la prestación de servicios médicos (Pacto Internacional de Derechos Económicos, Sociales, Culturales y Ambientales, 1976; Protocolo adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales "Protocolo de San Salvador", 1988). Sobre esta base, el derecho a la salud aplicaría a toda amenaza realizada mediante el uso de las nuevas tecnologías de la información, para lo cual se hace uso del principio de progresividad de los derechos humanos específicamente aplicado al desarrollo en el ámbito digital (Ávila, 2009, pp. 51-60).

Esto implica que la preparación de respuestas a incidentes informáticos que podrían afectar el derecho a la salud se debe construir desde una perspectiva de derechos humanos, que deben ser interpretados a la luz de la emergencia, de otros derechos y bienes jurídicos protegidos. De conformidad con los elementos de interpretación de la Convención Americana de Derechos Humanos (art. 29) y el Protocolo adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales, Culturales y Ambientales ("Protocolo de San Salvador", art. 10), es fundamental entender a la salud como un bien público, que si bien ha sido privatizado en gran parte en la región, es esencial para una respuesta transversal que atienda a eventuales vulnerabilidades de los sistemas de salud.

En este contexto, el Grupo de trabajo de Protocolo de San Salvador (2011) identificó seis dimensiones transversales en la construcción de indicadores y monitoreo sobre el derecho a la salud, las cuales son útiles para analizar las actuaciones ante la pandemia. En efecto, los Estados deben garantizar por un lado la accesibilidad a la salud, con una cantidad suficiente de bienes y servicios, así como la calidad de la misma lo cual implica la existencia de «equipo hospitalario científicamente aprobados y en buen estado» (p. 26).

Por ello, si bien estos estándares internacionales son adaptables a la situación de cada país, de manera general existe una obligación estatal de promover condiciones adecuadas para la provisión de servicios derivados del derecho a la salud. La Corte Constitucional del Ecuador (*Sentencia 904-12-JP/19*, 2019, pp. 10-12) considera que los estándares interamericanos y la Observación General 14 reconocen a la accesibilidad y a la calidad como elementos esenciales del derecho a la salud, que generan obligaciones directas a las instituciones públicas en el Ecuador. Esta visión también se plasma en la Constitución ecuatoriana (2008, art. 322), que contempla que

este derecho implica un acceso permanente y oportuno que se guíe bajo los principios de calidad y precaución.

Siguiendo la lógica interpretativa del bloque de constitucionalidad, lo anterior se complementa con la Corte Interamericana de Derechos Humanos que ratificó que la salud es un bien público que genera una obligación para el Estado «de prevenir que terceros interfieran indebidamente en el goce de los derechos a la vida y a la integridad personal, particularmente vulnerables cuando una persona se encuentra bajo tratamiento de salud» (*Caso Ximenes Lopes vs. Brasil*, 2006, § 88). Posteriormente, la misma Corte (*Caso Suárez Peralta vs. Ecuador*, 2013, § 132) amplió el deber del Estado hacia el establecimiento de un marco normativo que garantice la calidad de los servicios de salud y que prevenga cualquier amenaza a la integridad durante prestaciones sanitarias. Por aplicación del principio de progresividad (Ávila, 2009, p. 55) estas obligaciones implicarían que el Estado debe evitar la existencia de amenazas cibernéticas que podrían afectar la accesibilidad y la calidad del derecho a la salud en los hospitales en el Ecuador.

Sin embargo, el desarrollo interpretativo de los órganos de tratados del sistema universal de derechos humanos, o los parámetros de medición de avances en el cumplimiento del derecho a la salud en el sistema interamericano, no han contemplado la especificidad de la protección de facilidades médicas en el ciberespacio (Comité de Derechos Económicos, Sociales y Culturales, 2000). La extensión de las obligaciones de derechos humanos para la protección digital de los sistemas de salud podría ser cuestionada por la falta de una obligación específica para los Estados que no reconocen el valor de las interpretaciones de órganos de derechos humanos del sistema universal e interamericano en sus Estados. Ante la interconexión y multiplicidad de las amenazas, esta falta de obligaciones generalizadas de protección internacional genera brechas que permean los sistemas jurídicos internos, los cuales son incapaces de defenderse de manera individual ante ataques virtuales a sus sistemas de salud (Inversini, 2020, p. 268).

Empero, con fundamento en la obligación general de proteger en el DI-DDHH, el Comité de Derechos Económicos, Sociales y Culturales (2000) argumenta que los Estados tienen obligaciones extraterritoriales de hacer respetar el derecho a la salud con respecto a acciones que se originen en otros Estados y evitar, de esa manera, que terceros interfieran en su goce. Ahora bien, esta visión no deja de ser una interpretación que no goza de aplicación efectiva generalizada, salvo países que reconocen el valor vinculante de estos pronunciamientos, como lo afirma la Corte Constitucional del Ecuador (*Auto de verificación de sentencia No. 1470-14-EP/20*, 2020, p. 8). En efecto, los Estados en general no han aceptado una

obligación en la práctica o en sus declaraciones respecto al goce del derecho a la salud en terceros Estados.

De la misma manera, los Principios de Maastricht sobre la aplicación extraterritorial de las obligaciones en derechos económicos, sociales y culturales, proponen que los Estados suscriptores del PIDESC ya han aceptado una obligación de brindar cooperación internacional y asistencia en el cumplimiento de sus obligaciones de manera colectiva, inclusive el derecho a la salud (Fish, 2020). Según dicha visión, en la actualidad, los Estados gozarían de una obligación compartida en la división de la responsabilidad para responder a la pandemia por Covid-19. De ser el caso, el derecho a la salud estaría protegido de cualquier ataque a través del ciberespacio ante la obligación de los demás Estados colaborar en el cumplimiento del mismo.

Los Principios de Maastricht constituyen únicamente, por el momento, una declaración de *soft law* elaborada desde la academia universitaria, en base principalmente a las interpretaciones de los Comités de Derechos Humanos del sistema universal. Sin perjuicio de ello, es relevante que la Corte Constitucional del Ecuador, en 2010, haya reconocido a este tipo de instrumentos de *soft law*, sin ser vinculante, con un valor jurídicamente relevante para interpretar el alcance del contenido de los derechos (*Sentencia No.001-10-SIN-CC*, 2010, p. 58). Asimismo, esta Corte ha citado la Observación General No. 14 del Comité de Derechos Económicos, Sociales y Culturales para interpretar las obligaciones de los Estados en la protección del derecho a la salud (*Sentencia No. 904-12-JP/19*, 2019, p. 10). Los estándares emitidos por los Comités de Derechos Humanos del sistema universal generan un marco legal que por extensión amplía la protección del derecho a la salud al ciberespacio que resultaba aplicable en el Ecuador.

Sin embargo, la Corte Internacional de Justicia, en el caso Ahmadou Sadio Diallo, restó cualquier tipo de carácter jurídicamente vinculante a las interpretaciones de estos Comités, al considerar que solo pueden supervisar la aplicación de sus tratados y no generar obligaciones (*Caso Relativo a Ahmadou Sadio Diallo, Guinea v República Democrática del Congo*, 2010, § 66). Por lo tanto, si bien estas obligaciones extraterritoriales extensivas de los tratados internacionales sobre derechos económicos, sociales y culturales son aplicables al Ecuador, esto no es un reflejo de una percepción generalizada vinculante a nivel mundial. Ante la interdependencia de los Estados en el ciberespacio, la existencia de obligaciones de derechos humanos aisladas no genera un estándar de protección adecuado.

De la misma forma, Philip Alston, en su análisis plasmado en los *travaux préparatoires* del PIDESC, demuestra que la obligación del cooperación internacional del art. 2, carece de un carácter vinculante de

proveer cualquier tipo de asistencia (Alston, 1987, pp. 191-193). Así, los argumentos para demostrar que la protección de los sistemas de asistencia de salud estarían protegidos de ataques como parte de las obligaciones de cooperación internacional al amparo de los arts. 2 y 10 del PIDESC son débiles a nivel internacional. Además, de manera más reciente, ni los efectos devastadores del Covid-19 han movido la *opinio juris* de los Estados sobre la existencia de una obligación de cooperación al amparo del DI-DDHH en el ámbito de salud, inclusive si es concebida como una asistencia humanitaria por un desastre antrópico (Essawy, 2020).

Como una propuesta alternativa, Kubo Mačák argumenta la posible existencia de una obligación al amparo de los derechos civiles y políticos para la protección de los sistemas de asistencia de salud en el ciberespacio. Por ejemplo, en el caso de la interpretación del derecho a la vida, de acuerdo con el Comité de Derechos Humanos, los Estados tienen una obligación de proteger el derecho a la vida de manera extraterritorial en las operaciones llevadas a cabo por sus funcionarios. Sin embargo, este escenario solo cubriría los casos más extremos de una relación directa de una acción cibernética sobre la vida ajena, sin contemplar el rango de operaciones cibernéticas que pueden afectar los sistemas de asistencia de salud y de manera indirecta el derecho a la salud.

En este contexto, un enfoque de seguridad interna podría constituir un marco en el que generar respuestas de responsabilidad penal individual originada en el deber de garantía del DI-DDHH para los Estados. En efecto, a nivel interno en el Ecuador resulta aplicable el Código Orgánico Integral Penal (Código Integral Penal, 2014), que contempla la figura de asesinato «por cualquier otro medio» (art. 140) que arriesgue la salud de las personas. De la misma forma, constituye un agravante a las infracciones a la integridad que la víctima se encuentre en establecimiento de salud (art. 48). Sin embargo, estas obligaciones se aplican de manera territorial en el Ecuador y no implican una tipificación de las conductas que sean cometidas desde el exterior por medios cibernéticos en contra de la salud de una persona en el Ecuador. En efecto, los actores criminales operan en el ciberespacio desde diferentes ubicaciones y su infraestructura está desconcentrada sujeta a cambios constantes, lo que implica que cualquier enfoque puramente nacional está destinado al fracaso (Inversini, 2020, p. 268).

En este contexto, existen instrumentos internacionales como el Convenio de Budapest sobre ciberdelincuencia, adoptado en 2001 en el marco del Consejo de Europa, que incorporan un enfoque de tipificación y cooperación jurídica penal para ciberdelitos. Este Convenio, del cual no forma parte el Ecuador, aborda un enfoque de criminalización de conductas para individuos y normas para cooperación policial entre Estados (Consejo

de Europa, 2001, p. 2). Ahora bien, sin descartar que una posible ratificación del Convenio de Budapest pueda facilitar al Ecuador la armonización de su legislación en la materia, es posible que un marco normativo de esta naturaleza no llegue a colmar las lagunas existentes frente a las complejidades de la protección de facilidades médicas en el ciberespacio por la ambigüedad de las obligaciones extraterritoriales de los Estados con relación a los derechos a la salud y a la vida (Consejo de Europa, 2001, p. 37).

III.2. Aplicación general del Derecho internacional al ciberespacio, incluido el DI-DDHH en la protección del derecho a la salud

La visión propositiva de la reciente *Declaración de Oxford* supone la utilización en el espacio cibernético del Derecho internacional aplicable de manera tradicional al mundo físico, incluyendo también el DI-DDHH. De esta manera, el DI-DDHH aplicaría por un razonamiento de analogía al ciberespacio (D. Hollis, 2020, pp. 30-32) o por el recurso a principios generales del Derecho internacional a un nuevo escenario no contemplado en un inicio en la negociación de los tratados internacionales (Dinstein, 2013, p. 283).

Sin embargo, la aplicación del Derecho internacional tradicional, incluido el DI-DDHH, al ciberespacio está sujeta a constantes debates inter-estatales. Estas disquisiciones técnicas generan ciertos vacíos respecto a la protección del derecho a la salud en el ciberespacio. En efecto, si bien aún pueden existir dudas sobre el alcance de las obligaciones de DI-DDHH en la protección del derecho a la salud, la aplicación generalizada del Derecho internacional al ciberespacio podría suponer una solución.

Al respecto, a nivel de Naciones Unidas, actualmente avanzan los debates de dos mecanismos paralelos. Por un lado, el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (GGE) fue creado por la Resolución 73/266, adoptada por la Asamblea General de Naciones Unidas, la cual había sido presentada por Estados Unidos en noviembre de 2018 para renovar su mandato iniciado en 2004.

Por otro lado, actualmente sesiona el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones (OEWG), que proviene de la Resolución de la Asamblea General de Naciones Unidas 73/27, presentada anualmente por Rusia (Oficina de Asuntos de Desarme de las Naciones Unidas, 2019). En sus más recientes aportes escritos al OEWG, ciertos Estados como Países Bajos, Australia y Suiza, se refirieron de forma expresa a ataques al sector hospitalario y la explotación de la crisis del Covid-19 para emprender

operaciones cibernéticas, como un riesgo que demuestra de nuevo la urgente necesidad de clarificar la aplicación del Derecho internacional en el ciberespacio (Oficina de Asuntos de Desarme de las Naciones Unidas, 2020).

Sin embargo, en el desarrollo de los trabajos de ambos mecanismos de Naciones Unidas aún existe una brecha en la armonización de criterios relativos a la obligación de los Estados de abstenerse de atacar infraestructuras críticas de otros Estados, como las hospitalarias. Esto se debe precisamente a la inexistencia de un consenso mínimo sobre la definición de infraestructura crítica. Esta falta de una visión colectiva común, reflejada en la carencia de apoyos para adoptar el borrador de informe presentado por el GGE de 2016 y 2017 en la Asamblea General de Naciones Unidas, radica en la reticencia de los Estados a aceptar la aplicación del Derecho internacional a operaciones cibernéticas, con la paradójica excusa de ciertos países de es necesario evitar una militarización del ciberespacio (Sukumar, 2020).

Ante la falta de avances tangibles en Naciones Unidas, varios actores estatales y privados han propuesto diversas iniciativas con el fin de generar compromisos políticos referenciales para la protección de infraestructura civil crítica. Entre este tipo de iniciativas, en 2017 la empresa Microsoft lanzó el proyecto de una Convención Digital de Ginebra. Sin embargo, dicha iniciativa ha sido criticada por tratarse de una propuesta legalmente confusa, que carece del apoyo político estatal necesario y que se enfoca en un irreal consenso universal (NATO Cooperative Cyber Defence Centre of Excellence, 2018).

Adicionalmente, con un enfoque gradual, se destaca el lanzamiento del *Llamamiento de París* para la confianza y la seguridad en el ciberespacio, que tuvo lugar en noviembre de 2018. Se trata de una declaración política dirigida a proponer y reafirmar estándares mínimos de comportamiento y medidas de fomento de la confianza en la materia. Este documento político, respaldado hasta el momento por 78 Estados, reafirma la aplicación del DI-DDHH al ciberespacio. Además, afirma que los ciudadanos tienen los mismos derechos *off line* y *online* (Foro para la Gobernanza de Internet, 2018). No obstante, este documento es una declaración política sin valor jurídicamente vinculante, y su nivel de especificidad es aún muy reducido como para permitir una clarificación de la aplicabilidad del DI-DDHH en el espacio cibernético. El Ecuador no ha suscrito el *Llamamiento de París*.

A partir de la incertidumbre existente sobre la normativa aplicable para la protección en el ámbito digital, se mantiene aún el debate sobre si el DI-DDHH debe aplicarse por analogía al ámbito cibernético. En efecto, los instrumentos internacionales actuales podrían ser insuficientes para proteger

eficazmente los derechos humanos en el mundo virtual. Por este motivo, algunos autores llaman al reconocimiento de una cuarta ola de derechos humanos que incluiría un derecho a la seguridad informática vinculado con la paz cibernética (Riofrío, 2014, p. 40). En defensa de este derecho a una paz cibernética, Inversini (2020, p. 264) la concibe en su acepción negativa como la ausencia de guerra pero con un alto riesgo de violencia. Para avanzar de una paz negativa hacia una paz cibernética estable, la aplicación de los principios del DI humanitario, así como la generación de normas de comportamiento y un Derecho internacional que provoquen confianza y cooperación intergubernamental (2020, p. 268), para evitar ataques a infraestructura crítica que afecte a ciudadanos de otros Estados.

Sin embargo, otro debate para cubrir nuevos escenarios en el ciberespacio oscila entre la aplicación principios generales del Derecho Internacional o la generación de nueva normativa adaptada a las operaciones cibernéticas que atenten al derecho a la salud. De manera particular, las discusiones se enfocan en los intentos de crear normas internacionales para regular las actuaciones y operaciones llevadas a cabo en el plano del ciberespacio (Hollis, 2014, p. 18). Al respecto, aún existen retos vinculados con la fragmentación del Derecho internacional y el intento de extender el DI-DDHH y el DI humanitario existente al ciberespacio aún carece de soluciones o teorías unificadoras (Hollis, 2014, p. 20).

IV. DESAFÍOS DEL DI HUMANITARIO EN LA PROTECCIÓN DE LOS SISTEMAS DE ASISTENCIA DE SALUD EN EL CIBERESPACIO

En general, la exposición del sector salud a ataques directos o incidentales se incrementa por la interconectividad y progresiva digitalización a nivel global, sin distinción entre países. Esta nueva y compleja realidad compleja requiere debatir el alcance y la aplicación del DI humanitario en la protección de los sistemas de asistencia de salud en el ciberespacio (Ruhl, 2020). Sin embargo, desde el punto de vista jurídico, no es clara la manera de implementación del DI humanitario, pues aún ni siquiera existe un consenso internacional sobre el alcance de dicha implementación para guiar las acciones de los Estados.

Esta falta de claridad se refleja en el marco del trabajo que despliega el CICR con los Estados, en el ámbito de los foros multilaterales del sistema universal de Naciones Unidas, así como en la falta de éxito de declaraciones políticas recientes como el *Llamado de París* (Foro para la Gobernanza de Internet, 2018). Por consiguiente, varios autores han tratado de reordenar la interpretación de esta problemática actual a través de diversos acercamientos doctrinales.

Sobre la posición del CICR, cabe recordar que este organismo, en su análisis de noviembre de 2019 respecto a los principales retos contemporáneos del DI humanitario, ya había identificado al sector de la salud como uno de los más vulnerables. Además, un reconocido estudio del CICR sobre el DI humanitario consuetudinario (Henckaerts *et al.*, 2005, pp. 79-88), si bien puede ser cuestionado por su visión de *lege ferenda*, contempla la protección de los sistemas de asistencia de salud en cualquier conflicto armado con el rango de DI humanitario consuetudinario en las reglas 25 y 26. Para el CICR (2007, pp. 26-27), dicho sector de los sistemas de asistencia de salud se concibe como infraestructura civil crítica tomando en consideración el costo potencial de las operaciones cibernéticas.

Al respecto, la solución interpretativa que propone el CICR sobre esta nueva realidad de protección en el espacio cibernético parte del siguiente principio: el DI humanitario debe aplicarse por analogía a operaciones cibernéticas como a cualquier arma, medio o método de guerra, con un énfasis en el riesgo particular de ataques a los sistemas de asistencia de salud (Christory, 2019). Esta interpretación, que concuerda con su visión de reafirmar el respeto y vigencia del DI humanitario de manera general, fue planteada por el CICR en el marco de su declaración de diciembre de 2019 en el marco de la reunión del GGE.

No obstante, esta declaración realizada por el CICR generó fricciones entre los Estados, pues aún no se ha consolidado un consenso interestatal que permita afirmar que el DI humanitario es aplicable de manera directa al plano cibernético, entre otras razones por las dudas que existen sobre las implicaciones de que dicho reconocimiento podría proyectar en otras áreas del Derecho internacional (Sukumar, 2020). Por ejemplo, en las intervenciones de los Estados, estas reticencias se expresaron en la necesidad de evitar que la normativa del DI humanitario pueda expandirse al ejercicio del derecho a la legítima defensa consagrado en la Carta de las Naciones Unidas o en el plano de la retaliación a ataques cibernéticos con medios físicos (Ruhl *et al.*, 2020). En general, los Estados hasta el momento han evitado adoptar una visión específica o concreta que pudiera conducir en el futuro a una revitalización de la aplicación del DI humanitario al ciberespacio, ni mucho menos han previsto nuevas reglas que protejan claramente la infraestructura civil cibernética.

La doctrina iusinternacionalista, ante este panorama de falta de definiciones jurídicas, no ha encontrado tampoco aún un consenso sobre la posición que deba adoptarse. Para algunos autores, en medio de la incertidumbre sobre el alcance del DI humanitario en el espacio cibernético, se sostiene que una maleable interpretación del Derecho internacional podría incluso generar incentivos contraintuitivos al permitir o incluso exigir la

realización de operaciones cibernéticas. Por ejemplo, Noam Lubell (2012, p. 10), de manera alternativa a la visión del CICR, argumenta que si las operaciones cibernéticas no pueden ser calificadas como ataques bajo el DI humanitario, entonces no debería aplicarse el principio de distinción, por lo que se podría dirigir abiertamente agresiones contra elementos de infraestructura civil.

En este sentido, otros autores como Duncan Hollis (2014, pp. 30-32) argumentan que, de manera paradójica, al favorecerse una aplicación por analogía del DI humanitario caso por caso a conflictos cibernéticos, existiría un vínculo entre la extensión de los límites del DI humanitario y la existencia de un deber de *hackear*: de acuerdo con esta visión, los Estados estarían llamados a preferir el uso de operaciones cibernéticas cuando éste sea el medio menos gravoso para alcanzar un objetivo militar como extensión del principio de precaución. En contraste con esta postura, otra parte de la doctrina, como es el caso de Yoram Dinstein (2013, p. 283), cuestiona la visión de Hollis al considerar que su planteamiento no constituye un razonamiento analógico sino simplemente una aplicación de principios generales del DI humanitario a otro escenario diferente.

De la misma forma, en el plano doctrinal, y ante la falta de consensos y frente al subdesarrollo de un Derecho internacional que controle las operaciones cibernéticas, han surgido algunas iniciativas orientadas a regular el comportamiento de los Estados y a proteger ciertas facilidades civiles. Entre estas iniciativas académicas se destacan las dos versiones del *Manual de Tallinn* sobre el Derecho internacional aplicable a conflictos cibernéticos, desarrollado a título privado por un grupo de expertos y que constituye una referencia en la materia. En la primera versión del *Manual* se discuten las prohibiciones a ataques objetos civiles en el DI humanitario al amparo del art. 52 del Protocolo Adicional I a los Convenios de Ginebra (Schmitt, 2013, pp. 106-110). Sin embargo, inclusive dicho Manual, basándose en los comentarios de interpretación de los Protocolos Adicionales a los Convenios de Ginebra, expone las deficiencias, dificultades y debilidades a las que se enfrenta hoy en día la interpretación del Derecho aplicable a la protección de facilidades médicas en el ciberespacio como se analizará a continuación.

En este plano doctrinal, se exploran al menos cuatro problemáticas: el estatus de los datos digitales pertenecientes a infraestructuras civiles; la posible pérdida de protección por el carácter mixto de las facilidades que incluyen información virtual; y el momento a partir del cual se debe considerar aplicable el DI humanitario a en el espacio cibernético para la protección de los sistemas de asistencia de salud.

En primer lugar, en el análisis del costo potencial de las operaciones cibernéticas por parte del CICR existe una alta preocupación sobre la protección de datos civiles esenciales, tales como aquellos vinculados con unidades o facilidades médicas, y que se encuentran sujetos a múltiples amenazas en la actualidad (Gisel, 2018, p. 60). Este escenario se torna más complejo ante las amenazas cibernéticas enmarcadas en la respuesta a la pandemia por Covid-19. Al respecto, en su regla 30, el *Manual de Tallinn* concluye que los datos son intangibles y, por lo tanto, no pueden ser considerados como un objeto, por lo cual ciertos componentes de los sistemas de asistencia de salud podrían no ser considerados con la calidad de objetivo militar. Siguiendo este razonamiento, la destrucción de datos digitales almacenados o constituyentes de una infraestructura civil no estaría cubierta por el principio de distinción y, por tanto, no podrían constituir un objeto de ataque (Schmitt, 2013, p. 106). Esta perspectiva fue corregida parcialmente en la segunda versión del *Manual de Tallinn*, pues la regla 132 de esa versión contempla, al menos, que los sistemas de computación y los datos esenciales para el funcionamiento de las unidades médicas no podrían ser objeto de ataque (Schmitt, 2017b, p. 168).

En todo caso, como se señala en el informe de Duncan Hollis (2019, pp. 2-3), publicado en enero de 2019, sobre Derecho internacional y operaciones cibernéticas estatales de los miembros de la Organización de los Estados Americanos (OEA), debe advertirse la escasa aplicación práctica del *Manual de Tallinn*, en su primera y segunda versión. De la misma forma, la falta de pronunciamientos o práctica de los Estados sobre la aplicabilidad del Derecho internacional a operaciones cibernéticas es un problema común en la actualidad. Hollis reconoce, incluso, que los Estados que aceptan la importancia de aplicar ciertos elementos de Derecho internacional, mantienen aún amplias divergencias sobre su interpretación (Hollis, 2019, p. 4). De esta forma, la falta de consenso internacional sobre el alcance del concepto de objeto de ataque genera una importante brecha en la protección de los servicios de asistencia de salud a través de la exclusión de los datos esenciales civiles del ámbito de protección de objetos civiles en el DI humanitario, para este caso concreto (Hollis, 2019, p. 8).

En un segundo lugar, además de la disyuntiva mencionada sobre el estatus jurídico de los datos al amparo del DI humanitario en el ciberespacio, las redes civiles y militares pueden encontrarse interconectadas, razón por la cual una infraestructura en un principio civil puede llegar a perder la protección que en principio otorga el DI humanitario (Gisel & Rodenhäuser, 2020). En efecto, como argumenta Karinne Bannelier-Christakis en su interpretación del *Manual de Tallinn*, la civilinización de la guerra debido a conflictos asimétricos, el empleo de empresa militares y de nuevas

tecnologías ha logrado que el concepto de uso dual aumente los tipos de ataques autorizados contra objetos civiles (Bannelier-Christakis, 2015, p. 359).

De esta manera, la ambigüedad que suponen el ámbito de las operaciones cibernéticas, que pueden incluir ataques a facilidades que apoyan el esfuerzo de la guerra de manera indirecta, genera incertidumbre respecto a los umbrales de aplicación del principio de distinción sobre los objetos civiles, incluidos los sistemas de asistencia de salud (Bannelier-Christakis, 2015, p. 362). Este fenómeno se acentúa, además, con el actual proceso de securitización de la agenda de implementación de las políticas de protección de la salud ante la urgencia de respuestas inmediatas frente al Covid-19 (Walton, 2020). A esto, se suma la interconectividad de las redes informáticas y los debates sobre la soberanía con relación a los datos que transitan por otros países.

En tercer lugar, otro debate jurídico que surge es el siguiente: no es claro a partir de qué momento el DI humanitario debería ser aplicable en el espacio cibernético. Podría considerarse que si un ciberataque se realiza posteriormente a que tengan lugar operaciones cinéticas previas, el DI humanitario sí debe aplicarse. Bajo esta premisa, las operaciones cibernéticas serían una extensión o consecuencia de las otras (las cinéticas). Sin embargo, para llegar a esta conclusión, se requiere definir con anticipación si un ataque cibernético, como primer o único acto hostil, que no se encuentre vinculado a una acción física, puede considerarse por sí solo como el detonante para que el DI humanitario entre en aplicación (DeLuca, 2013, p. 304).

En este sentido, mayor complejidad aún reviste la atribución de responsabilidad internacional por la realización de operaciones cibernéticas con relación a actores no estatales. Máxime si se tiene en cuenta que tales operaciones podrían variar en una gama que iría desde la ignorancia de la conducción de operaciones desde su territorio, pasando por la instigación o, incluso, llegando a la situación en la que se produzca la dirección del ataque. Estas alternativas se basan en el proyecto de artículos sobre responsabilidad internacional de los Estados elaborados presentados ante la Asamblea General de Naciones Unidas por parte de la Comisión de Derecho Internacional (Iasiello, 2014, p. 58).

En cuarto lugar, los compromisos internacionales en derechos humanos podrían regular parcialmente la conducta de los Estados en la cibernética de los sistemas de asistencia de salud en el ciberespacio. Varios instrumentos internacionales han desarrollado el contenido del derecho humano a la salud cuyo contenido esencial lo caracteriza como un bien público que obliga al Estado a generar condiciones para asegurar la

prestación de servicios médicos (Pacto Internacional de Derechos Económicos, Sociales y Culturales, 1976, art. 12; Protocolo adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales "Protocolo de San Salvador", 1988, art. 10). En ese sentido, según la Asamblea General de Naciones Unidas (2014), la garantía y protección del derecho humano a disfrutar del derecho a la salud aplicaría en las mismas condiciones en el plano cibernético.

Sin embargo, el desarrollo interpretativo de los órganos de tratados del sistema universal de derechos humanos, o los parámetros de medición de avances en el cumplimiento del derecho a la salud en el sistema interamericano, no han contemplado la especificidad de la protección de facilidades médicas en el contexto de conflictos, menos aún en el ciberespacio (Grupo de Trabajo para el análisis de los informes nacionales del Protocolo de San Salvador, 2011; Comité de Derechos Económicos, Sociales y Culturales, 2000).

En suma, las visiones divergentes sobre la aplicabilidad del DI humanitario a operaciones cibernéticas, y la falta de consensos internacionales sobre las fronteras de aplicabilidad del DI humanitario a infraestructuras civiles generan vulnerabilidades e incertidumbres en la protección de los sistemas de asistencia de salud. Por ejemplo, los llamamientos internacionales a negociar y elaborar un instrumento internacional jurídicamente vinculante relativo a los sistemas de información en conflictos armados y operaciones cibernéticas, que incluya a Estados y actores no estatales, no han recibido un apoyo mayoritario hasta el momento (DeLuca, 2013, pp. 313-314).

Sin duda, la persistente indefinición sobre ciertos aspectos de la aplicación del DI humanitario al ciberespacio genera, por sí, un riesgo para los Estados en virtud de la falta de especificidad sobre las reglas que pueden aplicar en el caso de recibir un ataque y cuáles son los medios de respuesta idóneos. En ese sentido, debe recordarse que una correcta definición del DI humanitario produce un efecto potencial para afectar la concepción de las obligaciones de los Estados en tiempos de paz. A continuación, se analizará de qué manera estos debates son manejados desde la política exterior ecuatoriana con relación a la construcción del DI-DDHH y DI humanitario de manera contrastada con la visión de la protección de los sistemas de asistencia de salud a nivel interno.

V. DISONANCIA DISCURSIVA EN LA POLÍTICA EXTERIOR ECUATORIANA SOBRE LA PROTECCIÓN DEL DERECHO A LA SALUD EN EL CIBERESPACIO

La emergencia generada en 2020 por el Covid-19 renueva la necesidad de esclarecer el alcance y aplicabilidad de las normas de protección frente a operaciones cibernéticas para proteger los sistemas de asistencia de salud, especialmente en países pequeños o periféricos como Ecuador. En efecto, entre otras razones, la falta de claridad en la aplicación del DI-DDHH y DI humanitario para la protección del derecho a la salud y la infraestructura civil en el ciberespacio convierte al Ecuador en un país especialmente vulnerable ante la pandemia global del Covid-19.

Lejos de contribuir a despejar incertidumbres, los debates internacionales reseñados —la mayor parte de ellos aún sin una respuesta categórica— nublan aún más el ámbito de aplicación de la normativa para Estados que, como Ecuador, requieren proteger de manera efectiva sus sistemas de asistencia de salud, especialmente en situaciones de crisis o emergencia. Como consecuencia, parece estar produciéndose en Ecuador una disonancia discursiva entre la política exterior y la nacional con relación a la protección de los sistemas de asistencia de salud en el ciberespacio.

Como antecedente, debe recordarse que la posición ecuatoriana en materia de ciberseguridad se ha convertido en una prioridad nacional desde la segunda mitad de 2019. A la luz de los ataques cibernéticos supuestamente atribuidos a una reacción por el retiro, el 11 de abril de 2019, del asilo político reconocido al ciudadano Julian Assange en la Embajada en Londres, el Ecuador fortaleció las alianzas con organismos internacionales e incrementó la cooperación bilateral en esta materia. Esto significó una revitalización de su inserción en los debates multilaterales en materia de gobernanza en Internet y ciberseguridad (Frankz et al, 2019, p. 3).

Bajo este contexto, la posición que sostiene Ecuador en el ámbito multilateral que los procesos del GGE y del OEWG en el ámbito de Naciones Unidas no son excluyentes entre sí, sino complementarios, lo que ha significado el apoyo al trabajo en ambos espacios como una forma de asegurar y fortalecer la seguridad en el espacio cibernético (*Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, 2018, p. 4). En sus respectivas intervenciones en el OEWG, en septiembre de 2019 y febrero de 2020, Ecuador reconoció la importancia de la aplicación del Derecho internacional —incluidos el DI humanitario y el DI-DDHH— en el ciberespacio, desde el punto de vista de la generación de un marco normativo para el uso pacífico de este espacio (Gavrilovic & Stadnik, 2020).

Asimismo, en el marco de la OEA, solo Ecuador y Guyana enfatizaron la necesidad de contar un nuevo Derecho internacional en el contexto cibernético a inicios de 2020. En particular, Ecuador manifestó una posición favorable a establecer regulaciones sobre «los ataques a objetivos militares y/o civiles que afecten masivamente a la población, como es el caso de la infraestructura crítica, los hospitales (…) y otra infraestructura que afecte a la seguridad del Estado» (Hollis, 2020, p. 24).

Esta declaración muestra la conciencia de Ecuador de que es necesario proteger los sistemas de asistencia de salud de ataques cibernético. Sin embargo, también resalta la disonancia entre los pronunciamientos de política exterior y la normativa interna como se analiza a continuación. A la vez, estos pronunciamientos aislados resaltan la falta de consenso sobre la forma de avanzar en este proceso por parte de los Estados, a través de la aplicación de principios de Derecho internacional, incluido el DI humanitario y el DI-DDHH, o si es necesario un nuevo arreglo normativo.

No obstante, si bien las declaraciones ecuatorianas en los foros de Naciones Unidas y en el sistema Interamericano ratifican su voluntad de aplicar el DI humanitario y el DI-DDHH a operaciones cibernéticas (Oficina de Asuntos de Desarme de las Naciones Unidas, 2020), el manual de DI humanitario de las Fuerzas Armadas del Ecuador (2016, p. 30-35) no menciona el ámbito de aplicación de este régimen legal a operaciones cibernéticas, ni mucho menos su aplicabilidad con relación a infraestructura civil crítica tales como los sistemas de asistencia de salud

Esta disonancia discursiva sobre la aplicabilidad del DI humanitario y el DI-DDHH para el Ecuador genera incertidumbre respecto al marco legal de los sistemas de asistencia de salud en el espacio cibernético al no contar con un consenso sobre la interpretación de cómo se aplican estas normas entre Estados. Además, Ecuador aún no consta entre los países que respaldan el *Llamamiento de París* para la confianza y la seguridad en el ciberespacio de 2018 (Foro para la Gobernanza de Internet, 2018), lo que contraría la visión expresada en el CGE. Esta señal podría ser interpretada internacionalmente como un espacio de ambigüedad respecto a su posicionamiento sobre la aplicabilidad del DI humanitario y DI-DDHH a la protección del derecho a la salud y de la infraestructura crítica civil en el ciberespacio.

Para encontrar respuestas sobre la visión del Ecuador respecto a la aplicabilidad del DI humanitario a la protección de los sistemas de asistencia de salud en el ciberespacio, es necesario, por tanto, acudir a otros materiales. Por ejemplo, en su más reciente informe para la OEA, de marzo de 2020, Duncan Hollis (2020) compiló las respuestas de los Estados con relación a la aplicabilidad del Derecho internacional —incluidos el DI humanitario y

el DI-DDHH— a las operaciones cibernéticas y, por derivación, a la protección de la infraestructura de los sistemas de asistencia de salud. Este documento refleja la posición del Ecuador sobre este tema y permite a la vez reafirmar las complicaciones de aplicar normas originadas a inicios del siglo XX para la protección de bienes y personas civiles, a los desafíos de las nuevas tecnologías en el siglo XXI.

En efecto, sobre la definición de una operación cibernética bajo normas de DI humanitario, el Ecuador sostiene que la misma es operativa «en caso de dejar sin funcionalidad la infraestructura crítica del Estado» (Hollis, 2020, p. 17). Sin embargo, esta definición reafirma las debilidades identificadas en la falta de calificación de datos como objetos sin afectación a la funcionalidad de sistemas informáticos. Adicionalmente, ni Ecuador ni ningún otro Estado de la región apoyan la idea de aplicar el principio de distinción a datos civiles (Hollis, 2020, p. 18), lo cual constituye un punto primordial para la protección de los sistemas de asistencia de salud (Gisel, 2018, p. 19), reconocido como tal en la regla 132 del *Manual de Tallinn 2.0* (Schmitt, 2017b, p. 168). Asimismo, el marco normativo ecuatoriano no contempla aspectos para la catalogación y defensa de infraestructuras críticas cibernéticas nacionales pues «no existe un claro registro de la infraestructura crítica y, peor aún, de una definición de la información estratégica» (Vargas *et al.*, 2017, p. 38).

Sobre este marco legal, la *Política de la Defensa Nacional* de 2018, actualmente vigente, muestra varias deficiencias conceptuales con relación a la definición de amenazas y objetivos medibles para una política de planificación (Rivera, 2019). Además, su proyección de trabajo con miras al 2030, únicamente contempla la generación de una «capacidad considerable para defender la infraestructura crítica digital de las Fuerzas Armadas» (Ministerio de Defensa Nacional del Ecuador, 2019, p. 60). Esta concepción limitada se contrapone a la visión de la *Agenda Política de la Defensa 2014-2017*, que incluía como recursos estratégicos la información electrónica e infraestructura que afecta la seguridad integral del Estado y de los ciudadanos, incluido el ámbito sanitario (Ministerio de Defensa Nacional del Ecuador, 2014 pp. 55, 90-94).

En definitiva, el Ecuador se enfrenta a varios desafíos derivados, principalmente, de sostener internacionalmente una postura que no se ve inmediatamente reflejada en el plano doméstico. A ello se suma el hecho de que las dificultades conceptuales para incorporar normas difusas y tradicionales de DI humanitario que regulen las operaciones cibernéticas a nivel estatal, son exacerbadas por las lagunas internas respecto a la definición de infraestructura crítica, lo cual parece reducirse a objetivos militares. De esta manera, la ambigüedad de los parámetros para la

protección de infraestructura civil en el espacio cibernético, incluidos los sistemas de asistencia de salud, reitera la necesidad de clarificar el marco normativo sobre el Derecho internacional aplicable pues las falencias internas afectan la coherencia del discurso del Ecuador respecto a las normas de DI humanitario y DI-DDHH aplicables en el ciberespacio.

VI. CONSIDERACIONES FINALES

1. La protección jurídica del derecho a la salud y de los sistemas de asistencia de salud en el marco de la emergencia sanitaria por el Covid-19, permite reflexionar acerca de la extensión de la aplicación del DI-DDHH y DI humanitario desde una visión tradicional hacia el ciberespacio. Desde este punto de vista, cada vez es más evidente que el derecho a la salud genera una obligación jurídica del Estado de proteger a todos los ciudadanos en su territorio, que se extiende a la necesidad de adoptar medidas para evitar que terceros actores interfieran mediante ciberataques en el goce de dicho derecho.

2. La aplicación del principio de progresividad al derecho a la salud, entendido como un bien público, permitiría extender la protección jurídica no sólo a las instalaciones físicas, sino también a toda eventual amenaza digital. De conformidad con los estándares establecidos por mecanismos internacionales de derechos humanos del sistema universal e interamericano, la obligación de evitar ataques cibernéticos permite garantizar la calidad y continuidad de los servicios de salud. Sin embargo, el sistema de mecanismos de supervisión y vigilancia del cumplimiento de los tratados internacionales no se ha pronunciado de manera sistemática o específica sobre la protección del derecho a la salud en el ciberespacio.

3. Varias iniciativas de *soft law* han impulsado una interpretación de *lege ferenda* para proteger el derecho a la salud a partir de una obligación de cooperación internacional entre los Estados. De acuerdo a esta concepción, los Estados tendrían una responsabilidad compartida para proteger el derecho a la salud y protegerlo frente a cualquier ataque cibernético, en particular aquellos que se originen desde sus propios Estados hacia terceros mediante una obligación extraterritorial. Por ejemplo, a nivel nacional, la Corte Constitucional del Ecuador ha aceptado que estándares emitidos por los Comités de Derechos Humanos del sistema universal y estándares interamericanos, que reconocen a la accesibilidad y a la calidad como elementos esenciales del derecho a la salud, generan un marco legal que por extensión amplía la protección este derecho al ciberespacio. Desde este

punto, sería posible detectar la existencia de obligaciones directas a cargo de las instituciones públicas ecuatorianas.

4. Sin embargo, esa visión carece aún de un sustento legal, de una práctica consolidada y de un apoyo generalizado por parte de los Estados, tomando en consideración la falta de ratificación de ciertos instrumentos de derechos humanos y del reconcomiendo del valor del *soft law* como jurídicamente vinculante. De la misma forma, la protección del derecho a la salud derivada de una obligación extraterritorial de respeto del derecho a la vida en especial cibernético solo cubriría los casos más extremos.

5. Como alternativa, cabría pensar que un enfoque de seguridad interna y tipificación penal podría generar respuestas de responsabilidad penal originada en el deber de garantía del DI-DDHH. Sin embargo, las obligaciones contenidas en el Código Orgánico Integral Penal se aplican de manera territorial y no contemplan las conductas que sean cometidas desde el exterior por medios cibernéticos en contra de la salud en el Ecuador.

6. Adicionalmente, los actores criminales operan en el ciberespacio desde diferentes ubicaciones y su infraestructura está desconcentrada, sujeta a cambios constantes, lo que implica que cualquier enfoque puramente nacional esté destinado al fracaso. En este sentido, los esfuerzos de abordar la protección del derecho a la salud desde el ciberespacio a través de tratados internacionales de cooperación penal tampoco cubren las lagunas para una efectiva protección que defina claramente las obligaciones estatales.

7. Por su parte, desde la esfera de aplicación del DI-DDHH, incluso tomando en consideración varias propuestas normativas recientes, no ha logrado tampoco establecer en el plano normativo una forma de protección aceptada y efectiva por los Estados en el espacio cibernético tanto a las personas como a los sistemas de asistencia de salud.

8. Por analogía o por una aplicación de principios del Derecho internacional, varios autores y Estados alegan la obligación de aplicar sus disposiciones vigentes para operaciones cinéticas a aquellas en el ciberespacio. Sin embargo, esta visión está sujeta a constantes cuestionamientos en los debates inter-estatales sobre el alcance de las obligaciones de protección de los sistemas de asistencia de salud en el ciberespacio. Mientras estos debates se desarrollan, los vacíos en la protección de la salud se mantienen en el ciberespacio.

9. En este contexto, la falta de una visión colectiva, la ausencia de un consenso mínimo sobre la definición de obligaciones para la protección del derecho a la salud y los sistemas de asistencia de salud, así como la carencia de avances tangibles en el desarrollo del Derecho internacional en foros multilaterales no permiten clarificar el comportamiento responsable que deberían adoptar los Estados en el ciberespacio. El DI-DDHH y el DI

humanitario están sujetos a constantes debates que no permiten esclarecer las obligaciones de los Estados en la protección del derecho a la salud y los sistemas de asistencia de salud.

10. En el ciberespacio, es poco probable que el DI humanitario tenga fuerza normativa para constreñir las acciones de los Estados frente a la protección de la salud. No parece existir un compromiso robusto por el respeto de estas normas internacionales. Desde el ámbito jurídico, no existe una clara definición sobre el grado de aplicabilidad del DI humanitario al ciberespacio para guiar las acciones de los Estados. Las soluciones interpretativas del CICR de extender el DI humanitario tradicional ciberespacio no han ganado tracción con los Estados. En los foros multilaterales, en particular Naciones Unidas, los Estados han mostrado reticencia frente a esta interpretación. Desde el ámbito doctrinal, iniciativas como el *Manual de Tallinn*, han generado avances sobre el DI humanitario aplicable a operaciones cibernéticas, pero mantiene ciertas falencias interpretativas.

11. Varias dificultades persisten respecto a la protección y estatus de los datos digitales de infraestructura crítica, como en el caso de los sistemas de asistencia de salud. De la misma forma, surgen dificultades para definir el inicio de la aplicación del DI humanitario, generando incertidumbre sobre el momento en el cual los sistemas de asistencia de salud están protegidos por esa normativa. Ni siquiera existe un consenso sobre la forma de abordar y continuar con los debates, ya sea a través de una interpretación de tratados vigentes, una renovación de los compromisos, la emisión de declaraciones políticas o la generación de nuevos tratados de derecho internacional aplicables al ciberespacio. La falta de soluciones o teorías unificadores genera confusión a los Estados y, sobre todo, una falta de responsabilidad en la protección de la salud de sus ciudadanos.

12. A nivel nacional, las disonancias discursivas y normativas sobre la protección del derecho a la salud y los sistemas de asistencia de salud, desde el DI humanitario y el DI-DDHH, dificultan la comprensión del ámbito de aplicación al espacio cibernético, tanto a nivel interno, como en la posición del Ecuador sobre este tema en espacios multilaterales, en particular con relación a los foros del GGE y OEWG de Naciones Unidas, así como en la OEA. Lejos de contribuir a despejar incertidumbres, los debates internacionales reseñados —la mayor parte de ellos aún sin una respuesta categórica— nublan aún más el ámbito de aplicación de la normativa para Estados como el Ecuador. El Ecuador se enfrenta a varios desafíos derivados, principalmente, de sostener internacionalmente una postura que no se ve inmediatamente reflejada en el plano doméstico

respecto al ámbito de protección del derecho a la salud y de los sistemas de asistencia de salud.

13. La falta de consensos internacionales sobre el marco legal aplicable genera brechas a nivel de Estados —como Ecuador— en la regulación de la protección del derecho a la salud y los sistemas de asistencia de salud en el ciberespacio. La pandemia por Covid-19 no muestra señales de poder ser resuelta a corto plazo para los países en desarrollo. La presión operativa sobre los sistemas de salud podría tener un carácter sostenido. La protección del derecho a la salud y a los sistemas de asistencia de salud es esencial ante las implicaciones catastróficas que los ataques cibernéticos pueden tener para los Estados. Este tiempo de crisis podría ser una oportunidad: los Estados podrían aprovechar este momento para reafirmar y esclarecer sus compromisos sobre el Derecho internacional aplicable al ciberespacio. En este sentido, resulta oportuno repensar a la ciberseguridad como un asunto central de derechos humanos, esencial para proteger la salud.

14. Finalmente, en situaciones críticas, como la actual, la orientación de las decisiones institucionales que se adoptan en el presente tienen un impacto en el futuro, de manera que en un Estado puede tener lugar un agravamiento de los riesgos actuales al derecho a la salud y a los sistemas de protección de la salud, o una mejora de las condiciones de seguridad y salud de las personas más vulnerables (Klein, 2020).

REFERENCIAS

American College of Physicians-American Society of Internal Medicine. (1999). *No health insurance? It's Enough to Make You Sick—Scientific Research Linking the Lack of Health Coverage to Poor Health*. In https://www.acponline.org/acp_policy/policies/no_health_insurance_scientific_research_linking_lack_of_health_coverage_to_poor_health_1999.pdf.

Alston, P. (1987). The Nature and Scope of States Parties' Obligations under the International Covenant on Economic, Social and Cultural Rights. *Human Rights Quarterly*, *9* (2), 156-229. http://www.jstor.com/stable/762295

Asamblea Constituyente del Ecuador. Constitución de la República del Ecuador, Pub. L. No. Registro Oficial 449 (2008).

Asamblea General de las Naciones Unidas. *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional* (Informe de la Primera Comisión de Naciones Unidas A/73/505; Anuario de las Naciones Unidas sobre Desarme, pp. 6-8). (2018). https://doi.org/10.18356/dac57ff6-es

Asamblea General de las Naciones Unidas. Pacto Internacional de Derechos Económicos, Sociales y Culturales, Naciones Unidas, Serie de Tratados, 993, p. 3 (1976).

Asamblea General de las Naciones Unidas. *The right to privacy in the digital age* (A/RES/68/167). (2014). http://undocs.org/A/RES/68/167

Asamblea Nacional del Ecuador. Código Integral Penal, Pub. L. No. Registro Oficial Suplemento 180 (2014).

Ávila, R. (2009). Los principios de Aplicación de los Derechos. En *Nuevas instituciones del Derecho Constitucional ecuatoriano* (pp. 40-60). INREDH.

Bannelier-Christakis, K. (2015). Is the principle of distinction still relevent in Cyberwarfare? En *Research Handbook on International Law and Cyberspace, 15*, 343-365.

Bethlehem, D., & Lubell, N. (2012, octubre 1). Classification of Conflicts: The Way Forward. *International Law Meeting Summary*. International Law and the Classification of Conflicts, Londres.

Carrera, F., Quilligana, J., Aguilar, M. & Fiallos, S. (2019). Desafío de la ciberseguridad ante la legislación penal. *Revista Dilemas Contemporáneos*, VII, 1-16. https://doi.org/10.46377/dilemas.v31i1.1236

Cerda, H. (2002). *Los elementos de la investigación*. El Búho.

Christory, V. (2019). *Statetement "Cyber warfare: IHL provides an additional layer of protection"*. International Committee of the Red Cross. https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection

Clapham, A. (2007). *Human rights: A very short introduction*. Oxford University Press.

Comité de Derechos Económicos, Sociales y Culturales. (2000). *Observación general 14. El derecho al disfrute del más alto nivel posible de salud.* (E/C.12/2000/4, CESR).

Comité Internacional de la Cruz Roja. (2019). *International Humanitarian Law and Cyber Operations during Armed Conflicts*. [Submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security].

Comité Internacional de la Cruz Roja. Protocolo adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I), 1125 UNTS 3 (1978).

Comité Internacional de la Cruz Roja. Protocolo adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional (Protocolo II), 1125 UNTS 609 (1978).

Conferencia Diplomática para Elaborar Convenios Internacionales destinados a proteger a las víctimas de la guerra. Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña (Convenio I), (1950). https://www.icrc.org/es/doc/resources/documents/treaty/treaty-gc-1-5tdkna.htm

Conferencia Diplomática para Elaborar Convenios Internacionales destinados a proteger a las víctimas de la guerra. Convenio de Ginebra para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar (Convenio II), (1950). https://www.icrc.org/es/doc/resources/documents/treaty/treaty-gc-2-5tdkwc.htm

Conferencia Diplomática para Elaborar Convenios Internacionales destinados a proteger a las víctimas de la guerra. Convenio de Ginebra relativo a la protección debida a las personas civiles en tiempo de guerra (Convenio IV), (1950).

Consejo de Europa. Convenio sobre la ciberdelincuencia, Serie Tratados Europeos No.185 (2001).

Corte Constitucional del Ecuador. Auto de verificación de sentencia No. 1470-14-EP/20, Núm. 1470-14-EP (el 31 de julio de 2020). https://www.kimirina.org/images/kimirina/documentos/1470-14-EP-FINAL.pdf

Corte Constitucional del Ecuador. Sentencia No.001-10-SIN-CC, Casos No. 0008-09-IN y 0011-09-IN (2010).

Corte Constitucional del Ecuador. Sentencia No. 904-12-JP/19, (el 14 de septiembre de 2019).

Corte Interamericana de Derechos Humanos. Caso Suárez Peralta vs. Ecuador, (el 21 de mayo de 2013). https://www.corteidh.or.cr/docs/casos/articulos/seriec_261_esp.pdf

Corte Interamericana de Derechos Humanos. Caso Ximenes Lopes vs. Brasil, (el 4 de julio de 2006).

de Currea-Lugo, V. (2005). La salud como derecho humano. *Cuaderno Deusto de Derechos Humanos*, *32*, 29.

Corte Internacional de Justicia. (2010). Caso Relativo a Ahmadou Sadio Diallo, Guinea v República Democrática del Congo, ICGJ 428 (CIJ 2010) (Corte Internacional de Justicia el 30 de noviembre de 2010).

DeLuca, C. (2013). The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. *Pace International Law Review*, *3*(278), 39.

Dinstein, Y. (2013). Cyber War and International Law. *International Law Studies*, vol. 89, 276-287.

Essawy, R. (2020, abril 22). The Legal Duty to Cooperate amid Covid-19: A Missed Opportunity? *EJIL: Talk!* https://www.ejiltalk.org/the-legal-duty-to-cooperate-amid-covid-19-a-missed-opportunity/

Fish, T. (2020, abril 1). Covid-19 Symposium: Covid-19 Responses and State Obligations Concerning the Right to Health. *Opinio Juris*. http://opiniojuris.org/2020/04/01/covid-19-symposium-covid-19-responses-and-state-obligations-concerning-the-right-to-health-part-2/

Foro para la Gobernanza de Internet. (2018). *Llamamiento de París para la confianza y la seguridad en el ciberespacio*. Foro para la Gobernanza de Internet. https://pariscall.international/en/call

Fuerzas Armadas del Ecuador, Comando Conjunto. (2016). *Manual de Derecho Internacional Humanitario*. Resolución DBM-DOC-CCFFAA-05-2016. http://www.coed.mil.ec/archivos_coed/MANUAL%20DI humanitario.pdf

Gavrilovic, A., & Stadnik, I. (2020, septiembre 10). *Summary: 3rd Meeting of the first substantive session of the Open-Ended Working Group (OEWG)*. Digital Watch Observatory. https://dig.watch/resources/3rd-meeting-first-substantive-session-open-ended-working-group-oewg

Gisel, L. (2018). *The potential human cost of cyber operations* [Informe de reunión del Expertos del CICR]. Comité Internacional de la Cruz Roja.

Gisel, L., & Rodenhäuser, T. (2020, abril). Cyber operations and international humanitarian law: Five key points. *Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/

Grupo de Trabajo para el análisis de los informes nacionales del Protocolo de San Salvador. (2011). *Indicadores de progreso para medición de derechos contemplados en el Protocolo de San Salvador* (OEA/Ser.L/XXV.2.1). Secretaría de Desarrollo Integral, Organización de los Estados Americanos. https://www.oas.org/es/sadye/inclusion-social/protocolo-ssv/docs/indicadores-primer-agrupamiento.pdf

Henckaerts, J.-M., Doswald-Beck, L., Alvermann, C., & International Committee of the Red Cross (Eds.). (2005). *Customary international humanitarian law*. Cambridge University Press.

Hollis, D. (2014). Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack? *Cyberwar: Law & Ethics for Virtual Conflicts* [research paper], 1-53.

Hollis, D. (2019). *International Law and State Cyber Operations: Improving Transparency* (Third report. OEA/Ser.Q CJI/doc. 578/19). Organización de los Estados Americanos. https://www.oas.org/en/sla/iajc/docs/CJI_doc_578-19.pdf

Hollis, D. (2020). *Derecho Internacional y operaciones cibernéticas del Estado: Mejora de la transparencia* (OEA/Ser. Q CJI/doc. 603/20 rev.1; Cuarto informe.). Organización de los Estados Americanos. https://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1.pdf

Howell, P. (2020, septiembre 18). A patient has died after ransomware hackers hit a German hospital. *MIT Tecnnology Review*.

Hunt, P., & Backman, G. (2008, junio). Health systems and the right to the highest attainable standard of health. *Health and Human Rights*, *10* (1), 81-92. https://cdn1.sph.harvard.edu/wp-content/uploads/sites/2469/2013/07/7-Backman.pdf

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, *7*(1), 54-67. https://doi.org/10.5038/1944-0472.7.1.5

International Committee of the Red Cross. (2007). International humanitarian law and the challenges of contemporary armed conflicts: Document prepared by the International Committee of the Red Cross for the 30th International Conference of the Red Cross and Red Crescent, Geneva, Switzerland, 26-30 November 2007. *International Review of the Red Cross*, *89*(867), 719-757. https://doi.org/10.1017/S1816383107001294

Inversini, R. (2020). Cyber Peace: And How It Can Be Achieved. En M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity*. Springer International Publishing. Vol. 21. 259-276. https://doi.org/10.1007/978-3-030-29053-5_13

Klein, N. (2020, marzo 19). "Coronavirus Capitalism": Case for Transformative Change Amid Coronavirus Pandemic [Https://www.democracynow.org/2020/3/19/naomi_klein_coronavirus_capitalism]. *Democracy Now*. https://www.democracynow.org/2020/3/19/naomi_klein_coronavirus_capitalism

Mačák, K., Rodenhäuser, T., & Gisel, L. (2020, abril 2). Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections? *Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/

Ministerio de Defensa Nacional del Ecuador. (2014). *Agenda Política de la Defensa 2014-2017*.

Ministerio de Defensa Nacional del Ecuador. (2019). Política de la Defensa Nacional del Ecuador "Libro Blanco", Pub. L. No. Decreto Ejecutivo No. 633. https://www.cies.gob.ec/wp-content/uploads/2019/01/Libro-Blanco-Ministerio-de-Defensa.pdf

Müller, Á. (2014). El derecho a la salud y los derechos humanos. En M. Aizenberg (Ed.), *Estudios acerca del derecho de la salud*. Universidad de Buenos Aires. 15-73.

http://www.derecho.uba.ar/publicaciones/libros/pdf/estudios-acerca-del-derecho-de-la-salud/estudios-derecho-de-salud-marisa-aizenberg.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2018, septiembre). Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/news/2017/geneva-conventions-apply-to-cyberspace-no-need-for-a-digital-geneva-convention/

Oficina de Asuntos de Desarme de las Naciones Unidas. (2019). *Developments in the field of information and telecommunications in the context of international security*. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

Oficina de Asuntos de Desarme de las Naciones Unidas. (2020). Open-ended Working Group: Comments by Member States on the initial pre-draft of the OEWG report. *Oficina de Asuntos de Desarme de las Naciones Unidas*. https://www.un.org/disarmament/open-ended-working-group/

Okande, D., Hollis, D., Koh, H., & O'Brien, J. (2020, mayo 21). Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector [Oxford Institute for Ethics, Law and Armed Conflict]. *Opinio Juris*. https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea

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

Organización de los Estados Americanos. (1988). Protocolo adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales "Protocolo de San Salvador".

Presidencia de la República de Ecuador. (2020, marzo 16). *El presidente Lenín Moreno decreta Estado de Excepción para evitar la propagación del Covid-19.* Secretaría General de Comunicación. https://www.comunicacion.gob.ec/el-presidente-lenin-moreno-decreta-estado-de-excepcion-para-evitar-la-propagacion-del-covid-19/

Riofrío, J. C. (2014). La cuarta ola de derechos humanos: Los derechos digitales. *Revista Latinoamericana de Derechos Humanos*, 25 (1), 15-45.

Rivera, F. (2019, enero 16). ¿Qué tan nueva es la actual Política de la Defensa? *Plan V*. https://www.planv.com.ec/historias/sociedad/que-tan-nueva-la-actual-politica-la-defensa

Ruhl, C. (2020, abril 6). *Note to Nations: Stop Hacking Hospitals*. Foreign Policy. https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/

Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020, febrero 26). *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Carnegie Endowment For International Peace. https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110

Sarat, A., & Lezaun, J. (eds.). (2009). *Catastrophe: Law, politics, and the humanitarian impulse*. University of Massachusetts Press.

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. http://dx.doi.org/10.1017/CBO9781139169288

Schmitt, M. (2017a). Grey Zones in the International Law of Cyberspace. *Yale Journal of International Law*, 42 (2), 1-27.

Schmitt, M. (2017b). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (2a ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Shackelford, S. (2017). Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace. *Stanford Journal of International Law.* No. 2019. 17-55. http://dx.doi.org/10.2139/ssrn.3005062

Sukumar, A. (2020, abril 17). The UN GGE Failed. Is International Law in Cyberspace Doomed As Well? *Lawfare*. https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well#

Vargas, R., Reyes, R. P., & Recalde, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, 20, 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Walton, C. (2020, abril 3). *Spies Are Fighting a Shadow War Against the Coronavirus*. Foreign Policy. https://foreignpolicy.com/2020/04/03/coronavirus-pandemic-intelligence-china-russia/

Zibel, M. (2019, octubre 5). Estado de excepción en Ecuador: Por qué continúa el conflicto pese al levantamiento del paro nacional de transportistas. *BBC Mundo*. https://www.bbc.com/mundo/noticias-america-latina-49944211

Zibel, M. (2020, abril 26). Coronavirus en Ecuador: La tragedia de las familias de Guayaquil que no encuentran a sus muertos. *BBC Mundo*. https://www.bbc.com/mundo/noticias-america-latina-52407158