Cuadernos de Nuestra América/Nueva Época/No. 010 / enero-marzo 2024/
RNPS: 2529 /ISSN: 2959-9849/99 pp.

Aplicación del Derecho Internacional en el Ciberespacio

Application of International Law in Cyberspace

Recibido: enero 2024.
Aprobado: febrero 2024.

Ms.C. Emilio Horacio Valencia Corozo

Instituto de Altos Estudios (IAEN), Quito, Ecuador.
ORCID: 0009-0007-5886-1267.
Email: emiliohoracio1@hotmail.com

Resumen

El contexto actual está marcado por el avance tecnológico y la creciente dependencia de la sociedad en el ciberespacio. El aumento del uso de internet y de las redes digitales ha planteado nuevos desafíos en términos de regulación y aplicación del derecho internacional. Por tanto, es necesario analizar cómo se aplica el derecho internacional en el ciberespacio. La pregunta científica que guía esta investigación es: ¿Cuáles son las aplicaciones del derecho internacional en el ciberespacio? El objetivo general consiste en analizar cómo se aplica el derecho internacional en el ciberespacio y determinar cuáles son las principales implicaciones que este tiene en la esfera digital. La metodología utilizada en este estudio se basa en el paradigma cualitativo, específicamente en la revisión documental. Se realizó una búsqueda exhaustiva de textos académicos y legales relevantes que abordaran el tema de la aplicación del derecho internacional en el ciberespacio. Se seleccionaron aquellos que proporcionaran información valiosa sobre las aplicaciones prácticas del derecho internacional en este ámbito. Los hallazgos de esta investigación revelan que la aplicación del derecho internacional en el ciberespacio es un tema complejo y en constante evolución. Se encontró que existen diferentes enfoques y perspectivas en cuanto a la forma en que se debe aplicar el derecho internacional en el ámbito digital. Algunos defienden la necesidad de adaptar el derecho internacional existente a las particularidades del ciberespacio, mientras que otros abogan por la creación de un marco legal específico para regular las actividades en línea. En cuanto a las conclusiones, se puede afirmar que el derecho internacional tiene un papel fundamental en la regulación y aplicación de normas en el ciberespacio. Sin embargo, existe la necesidad de adaptar y actualizar el derecho internacional para abordar los desafíos y las realidades del mundo digital. Además, se requiere una mayor cooperación y coordinación a nivel internacional para asegurar una aplicación efectiva del derecho en el ciberespacio.

Palabras clave: *Ciberseguridad, Privacidad, Jurisdicción, Derecho internacional, Cooperación internacional.*

Abstract

The current context is marked by technological advancements and society's increasing dependence on cyberspace. The rise in internet usage and digital networks has presented new challenges in terms of regulating and applying international law. Therefore, it is necessary to analyze how international law is applied in cyberspace. The scientific question guiding this research is: What are the applications of international law in cyberspace? The general objective is to analyze how international law is applied in cyberspace and determine the main implications it has on the digital sphere. The methodology used in this study is based on the qualitative paradigm, specifically on documentary review. A thorough search was conducted for relevant academic and legal documents that addressed the topic of the application of international law in cyberspace. Those documents were selected that provided valuable information on the practical applications of international law in this field. The findings of this research reveal that the application of international law in cyberspace is a complex and constantly evolving topic. It was found that there are different approaches and perspectives regarding how international law should be applied

in the digital realm. Some argue for the need to adapt existing international law to the particularities of cyberspace, while others advocate for the creation of a specific legal framework to regulate online activities. In terms of conclusions, it can be stated that international law plays a fundamental role in regulating and applying norms in cyberspace. However, there is a need to adapt and update international law to address the challenges and realities of the digital world. Additionally, greater international cooperation and coordination are required to ensure effective application of law in cyberspace.

Keywords: *Cybersecurity, Privacy, Jurisdiction, International law, International cooperation.*

Introducción

El contexto de la aplicación del derecho internacional en el ciberespacio se desarrolla en un entorno digital globalizado y en constante evolución. El ciberespacio se ha convertido en una dimensión fundamental de la sociedad moderna, donde se llevan a cabo diversas actividades, como la comunicación, el comercio electrónico, la banca en línea, el entretenimiento y la interacción social. Sin embargo, este entorno digital también ha dado lugar a una serie de desafíos y problemas que requieren una atención especial desde la perspectiva del derecho internacional.

Uno de los principales desafíos es que las actividades en línea no están limitadas por las fronteras geográficas, lo que plantea dificultades para la aplicación de las leyes nacionales tradicionales.

En este marco también es un desafío, determinar quién es responsable de las acciones ilegales en el ciberespacio, aspecto que resulta complicado debido a la capacidad de ocultar la identidad y la ubicación física mediante el uso de tecnologías de anonimato y técnicas de hacking sofisticadas. Otro aspecto importante del contexto es el conflicto de normas y regulaciones (Dinstein, 2018). Dado que el ciberespacio es un entorno transnacional, diferentes países tienen diferentes marcos legales y regulaciones en relación con el uso de Internet y la tecnología digital. Esto genera conflictos y desacuerdos sobre asuntos como la privacidad, la protección de datos, la libertad de expresión y el acceso a la información.

El resultado es que existe un debate sobre si los Estados tienen autoridad para regular y controlar actividades en línea que afectan a sus ciudadanos o infraestructura digital. Además, se plantea la cuestión de cómo responsabilizar y prevenir actividades perjudiciales en el ciberespacio. También existen desacuerdos sobre cómo equilibrar la protección de la privacidad con la necesidad de garantizar la seguridad en línea. Además, se enfrentan desafíos para definir y abordar los ataques cibernéticos, así como para desarrollar normas y tratados internacionales en ciberseguridad (Brownlie, 2008).

La aplicación del derecho internacional en el ciberespacio presenta varias contradicciones teóricas, metodológicas y prácticas, que reflejan los desafíos y complejidades inherentes a la regulación de un entorno digital global. Desde el punto de vista teórico, la contradicción radica en la dificultad de aplicar el derecho internacional tradicional, diseñado principalmente para regular las relaciones entre Estados en el ámbito físico, al ciberespacio. El ciberespacio no está limitado por fronteras geográficas y plantea desafíos únicos que no se ajustan fácilmente a los marcos legales existentes. Esto ha llevado a debates sobre si se necesita un conjunto de normas y principios específicos para el ciberespacio o si se pueden aplicar las normas y principios existentes de manera adecuada.

Metodológicamente, existen desafíos de establecer mecanismos efectivos para hacer cumplir el derecho internacional en el ciberespacio. Dado que el ciberespacio es un espacio virtual donde las actividades pueden ser anónimas y transfronterizas, resulta complicado identificar y responsabilizar a los infractores. Además, la rápida evolución de la tecnología y las tácticas utilizadas por los actores malintencionados dificulta la adaptación de los marcos legales y los enfoques de aplicación existentes.

En la práctica existen tensiones entre la necesidad de garantizar la seguridad y la protección de los Estados y los individuos en línea, y el respeto a los derechos humanos, como la privacidad y la libertad de expresión. El hecho es que las diferencias en las leyes y regulaciones nacionales, así como en los intereses y capacidades de los Estados, dificultan la cooperación internacional efectiva en la aplicación del derecho internacional en el ciberespacio.

A partir del análisis anterior, el problema a resolver en el contexto de la aplicación del derecho internacional en el ciberespacio, radica en la falta de un marco normativo claro y efectivo, así como en la insuficiente cooperación internacional. Abordar estos problemas es esencial para garantizar la protección de los derechos en línea, fortalecer la ciberseguridad y promover la estabilidad y la gobernanza efectiva del ciberespacio. Por lo tanto, el objetivo de esta investigación es analizar la aplicación del derecho internacional en el ciberespacio, examinando los desafíos, las contradicciones y los avances en este campo, con el fin de comprender su relevancia y ofrecer posibles enfoques para una regulación efectiva y equilibrada.

Hipótesis: La hipótesis planteada es que la aplicación efectiva del derecho internacional en el ciberespacio requiere el desarrollo de un marco normativo específico y la promoción de una mayor cooperación y colaboración internacional. El ciberespacio ha presentado desafíos significativos para la aplicación del derecho internacional debido a su naturaleza transfronteriza y su rápida evolución tecnológica.

Para abordar esta hipótesis, es esencial examinar las contradicciones y los avances en el campo de la regulación del ciberespacio, así como las iniciativas existentes para fortalecer la aplicación del derecho internacional en este ámbito (United Nations General Assembly. 2015). El desarrollo de un marco normativo específico para el ciberespacio es fundamental para superar las contradicciones teóricas y metodológicas. Este marco debería abordar las cuestiones únicas del ciberespacio, como la seguridad cibernética, la protección de datos, la privacidad y la responsabilidad de los actores estatales y no estatales.

La Convención de Budapest sobre Cibercrimen es un ejemplo de un tratado internacional que aborda algunos de estos aspectos (United Nations Office on Drugs and Crime, 2001). Sin embargo, se necesita una mayor cooperación y consenso para desarrollar un marco más integral y actualizado. La cooperación y colaboración internacional también son fundamentales para la aplicación efectiva del derecho internacional en el ciberespacio. Dado que las actividades cibernéticas pueden trascender las fronteras nacionales, la cooperación entre los Estados es esencial para investigar y enjuiciar a los infractores.

Además, la colaboración entre los Estados, la sociedad civil y el sector privado es crucial para intercambiar información relevante, desarrollar capacidades conjuntas y promover mejores prácticas en materia de ciberseguridad y protección de datos (Schmitt, et al., 2019). El papel de las organizaciones internacionales y los foros multilaterales, como las Naciones Unidas y el Foro de Gobernanza de Internet, también es importante en la promoción de la aplicación del derecho internacional en el ciberespacio (DeNardis, 2014). Estas plataformas proporcionan espacios para el diálogo, la cooperación y la elaboración de normas y principios comunes.

El tema de la aplicación del derecho internacional en el ciberespacio es de suma importancia debido a la falta de límites geográficos en este ámbito, lo que plantea desafíos para su regulación. Además, la existencia de amenazas como ciberataques y el robo de datos requiere una aplicación efectiva para fortalecer la ciberseguridad y proteger los derechos de los individuos en línea. También es importante garantizar la protección de datos personales y la privacidad en el ciberespacio, así como fomentar la cooperación internacional para enfrentar los desafíos transfronterizos. En resumen, la aplicación del derecho internacional en el ciberespacio es fundamental para promover la estabilidad, seguridad y gobernanza global en este ámbito.

Derecho internacional y ciberespacio: conceptos de partida

El derecho internacional es un conjunto de normas y principios que regulan las relaciones entre los Estados y otros actores internacionales en la comunidad internacional (Rosenzweig, & Nakatani, 2017). También se conoce como derecho de las naciones o derecho de las relaciones internacionales. Estas normas y principios están destinados a regular diversos aspectos de las relaciones internacionales, como la solución de disputas, los derechos humanos, el comercio internacional y el uso de la fuerza.

El ciberespacio, por su parte, se refiere al entorno digital en el que se llevan a cabo actividades en línea. Es un espacio virtual interconectado que permite la comunicación, el intercambio de información y la realización de transacciones a través de redes de computadoras en todo el mundo. El ciberespacio no está limitado por fronteras geográficas y abarca una amplia gama de actividades, como el comercio electrónico, las redes sociales, la banca en línea y la comunicación por correo electrónico (Schmitt, 2013)

El derecho internacional y el ciberespacio están interrelacionados debido a la creciente importancia de la regulación de las actividades en línea en el ámbito global. A medida que las interacciones en el ciberespacio se vuelven más frecuentes y relevantes, surgen desafíos legales relacionados con la privacidad, la seguridad cibernética, la protección de datos y la responsabilidad de los actores estatales y no estatales. El derecho internacional tiene como objetivo abordar estos desafíos y establecer normas y principios que rijan la conducta de los Estados y otros actores en el ciberespacio.

Avances del derecho internacional en el ciberespacio

El avance del derecho internacional en el ciberespacio ha sido un tema en constante evolución debido al rápido desarrollo de las tecnologías de la información y la comunicación, ello es palpable en lo siguiente (DeNardis, 2014, Dinstein, 2018 y Schmitt, & Vihul, 2019):

Marco normativo: Se ha trabajado en la creación de marcos normativos internacionales para regular las actividades en el ciberespacio. Uno de los principales instrumentos es la Convención sobre Cibercriminalidad del Consejo de Europa, que establece medidas para combatir los delitos informáticos a nivel internacional.

Responsabilidad estatal: Se ha reconocido que los Estados tienen la responsabilidad de prevenir y responder a los ciberataques que provengan de su territorio o que estén dirigidos contra otros Estados. Los ataques cibernéticos pueden ser considerados una violación de la soberanía de un Estado y, en algunos casos, incluso un acto de guerra.

Protección de datos: Con el creciente intercambio de información personal en línea, ha surgido la necesidad de proteger los datos en el ciberespacio. Varios tratados y convenios internacionales, como el Reglamento General de Protección de Datos de la Unión Europea, establecen estándares para la protección de la privacidad y la seguridad de los datos personales.

Ciberdelincuencia transfronteriza: El ciberespacio permite la comisión de delitos sin necesidad de cruzar fronteras físicas. Por lo tanto, se han establecido mecanismos de cooperación internacional para investigar y enjuiciar a los delincuentes cibernéticos. Además de la Convención sobre Cibercriminalidad, existen otros acuerdos regionales y bilaterales que facilitan la cooperación y el intercambio de información entre los Estados.

Defensa cibernética: Los Estados han desarrollado capacidades defensivas en el ciberespacio para proteger su infraestructura crítica y sus sistemas de información. Esto implica la toma de medidas para prevenir y responder a los ciberataques, además de la cooperación con otros Estados y organizaciones internacionales.

Ciberseguridad: El derecho internacional también ha avanzado en materia de ciberseguridad, con el fin de proteger a los usuarios individuales y a las organizaciones de los riesgos cibernéticos. Se han promovido iniciativas para la concienciación, la capacitación y la adopción de medidas de seguridad en el ciberespacio.

Amenazas y riesgos en el ciberespacio

A pesar de que existen avances, todavía en el ciberespacio, existen diversos riesgos y amenazas que plantean desafíos significativos en términos de seguridad, privacidad y estabilidad.

El Cibercrimen abarca actividades delictivas en línea, como el fraude financiero y el robo de identidad. Según el Informe de Ciberseguridad de Cisco 2021, el costo global del cibercrimen ascendió a aproximadamente 6 billones de dólares en 2020. Además, se estima que los incidentes de phishing aumentaron en un 220% durante la pandemia de Covid-19, aprovechando la incertidumbre y el aumento del trabajo remoto (Cisco, 2021).

Los ataques cibernéticos, como los ataques de ransomware y las intrusiones en sistemas gubernamentales, representan una amenaza para la infraestructura y los servicios en línea. Un ejemplo destacado es el ataque de ransomware a la empresa Colonial Pipeline en 2021, que interrumpió el suministro de combustible en gran parte de la costa este de Estados Unidos. Este incidente resaltó la vulnerabilidad de las infraestructuras críticas frente a los ataques cibernéticos.

La desinformación y la propagación de narrativas engañosas en línea pueden influir en la opinión pública y socavar la estabilidad política. Durante las elecciones presidenciales de Estados Unidos en 2016, se

identificaron campañas de desinformación y propaganda impulsadas por actores extranjeros en las redes sociales, con el objetivo de influir en la percepción y el proceso electoral.

La recopilación masiva de datos y la vigilancia en línea plantean preocupaciones sobre la privacidad y la confidencialidad de la información personal. Por ejemplo, en 2018, se reveló que la empresa Cambridge Analytica había obtenido ilegalmente datos de millones de usuarios de Facebook, lo que generó un debate sobre la protección de la privacidad y el uso indebido de datos personales (Cadwalladr, 2018).

Comprendiendo los desafíos a los que se enfrenta la regulación del ciberespacio

Por otro lado, la regulación del ciberespacio enfrenta una serie de desafíos debido a la naturaleza transnacional y dinámica de las actividades en línea: En términos de jurisdicción y soberanía, el ciberespacio no está limitado por fronteras geográficas, lo que dificulta la aplicación efectiva de la regulación nacional. Los delitos cibernéticos pueden originarse en un país y afectar a otros, lo que plantea desafíos en términos de jurisdicción y coordinación internacional. La determinación de qué jurisdicción tiene autoridad sobre un delito en línea y cómo se puede hacer cumplir la ley en un entorno transfronterizo es un desafío complejo (DiResta, & Shaffer, 2018).

Se suma que las tecnologías y las amenazas cibernéticas evolucionan rápidamente, lo que dificulta la capacidad de los marcos regulatorios para mantenerse actualizados. Los delincuentes cibernéticos pueden aprovechar las lagunas existentes en la regulación y adaptarse rápidamente a las contramedidas implementadas, lo que dificulta la detección y prevención de actividades ilícitas en línea.

Una particularidad del ciberespacio es que permite el anonimato y la dificultad de atribuir actividades a actores específicos (Goldsmith, & Wu, 2006). Esto plantea desafíos para la identificación y responsabilización de los perpetradores de delitos en línea. La capacidad de ocultar la identidad y utilizar técnicas de enmascaramiento dificulta la aplicación de la ley y la búsqueda de la responsabilidad penal. Por lo tanto, la regulación del ciberespacio requiere una cooperación y coordinación efectivas entre los Estados y actores internacionales.

Sin embargo, los intereses nacionales y las diferencias en las leyes y normas pueden dificultar la armonización de los enfoques regulatorios. La falta de consenso sobre los estándares y principios clave puede generar lagunas y obstáculos en la regulación del ciberespacio (Kshetri, 2017).

Vacíos legales en el marco jurídico internacional

El marco jurídico internacional relacionado con el ciberespacio enfrenta vacíos legales y lagunas significativas debido a la naturaleza transnacional y en constante evolución de las actividades en línea. Algunas áreas donde las normas y tratados existentes pueden resultar insuficientes para abordar los desafíos son las siguientes (Schmitt, & Vihul, 2019, UN General Assembly, 2015):

En relación a la atribución y responsabilidad, el anonimato y la dificultad de atribuir actividades en línea a actores específicos plantean desafíos para la responsabilidad legal. La falta de mecanismos efectivos de atribución dificulta la identificación y persecución de los responsables de delitos cibernéticos. Además, la ciberdelincuencia a menudo cruza fronteras, lo que dificulta la aplicación de la ley y la cooperación internacional.

Sobre la jurisdicción y extraterritorialidad, el ciberespacio no reconoce fronteras geográficas, lo que crea desafíos para la aplicación de la ley y la jurisdicción. Los delitos cibernéticos pueden originarse en un país, afectar a otros y utilizar infraestructuras ubicadas en múltiples jurisdicciones. Esto puede generar conflictos de jurisdicción y dificultades en la cooperación para llevar a los delincuentes ante la justicia.

Existe una falta de consenso internacional sobre las normas y estándares en el ciberespacio. Los países tienen diferentes enfoques y marcos legales para abordar los desafíos cibernéticos, lo que puede generar lagunas y dificultades en la cooperación. La falta de armonización puede obstaculizar la aplicación efectiva de la ley y la respuesta coordinada a las amenazas en línea.

Las rápidas innovaciones tecnológicas superan la capacidad de los marcos legales existentes para mantenerse al día. Las nuevas tecnologías, como la inteligencia artificial, el aprendizaje automático y la computación en la nube, plantean desafíos únicos que pueden requerir enfoques legales y regulatorios específicos. La adaptación de las leyes existentes para abordar estos avances tecnológicos puede resultar lenta y limitada.

Creación de marcos legales adecuados ¿Cómo adaptar el derecho internacional existente para abordar los desafíos del ciberespacio?

La adaptación del derecho internacional existente para abordar los desafíos del ciberespacio es un tema complejo y en constante evolución que requiere el examen de tratados y convenios existentes, así como la evaluación de su aplicabilidad y relevancia en el contexto digital. Ejemplos relevantes son (Consejo de Europa, 2004, Naciones Unidas,1961):

Convención de Budapest sobre Cibercrimen

Adoptada en 2001, esta convención se centra en la armonización de la legislación nacional para combatir delitos informáticos, como el acceso no autorizado, el daño a sistemas informáticos y la interferencia en datos. Es un tratado internacional que tiene como objetivo abordar el Cibercrimen, incluyendo delitos como el acceso ilegal a sistemas informáticos, el fraude informático y el abuso de dispositivos informáticos.

Este tratado establece medidas para fortalecer la cooperación internacional en la investigación y persecución de delitos cibernéticos, así como para promover la armonización de las leyes nacionales en este ámbito. Si bien la Convención de Budapest es relevante en el ámbito de la ciberseguridad y la lucha contra el Cibercrimen, su aplicación puede variar según la jurisdicción y la capacidad de los países para implementar sus disposiciones. La Convención de Budapest es un ejemplo de cómo el derecho internacional existente puede adaptarse para abordar los delitos en línea y promover la cooperación entre los Estados.

En el contexto digital actual, la Convención de Budapest sigue siendo relevante y aplicable, ya que los delitos cibernéticos continúan siendo una amenaza importante. Sin embargo, es importante adaptarla para abordar nuevos tipos de delitos cibernéticos que han surgido desde su adopción, como los ataques cibernéticos a infraestructuras críticas y la propagación de desinformación en línea.

Convención de Viena sobre Relaciones Diplomáticas

Por otro lado, la Convención de Viena sobre Relaciones Diplomáticas, adoptada en 1961, es un tratado que establece las normas y principios para las relaciones diplomáticas entre los Estados. Aunque esta convención no fue diseñada específicamente para el contexto digital, muchos de sus principios siguen siendo relevantes (Naciones Unidas, 1961). Por ejemplo, el principio de inviolabilidad de las comunicaciones diplomáticas puede aplicarse a las comunicaciones en línea de las misiones diplomáticas.

Sin embargo, es importante reconocer que la evolución de las tecnologías de la información y la comunicación plantea nuevos desafíos, como la seguridad de las comunicaciones digitales y la protección de la información sensible en línea, que pueden requerir ajustes y actualizaciones en el marco legal existente.

Es fundamental realizar una evaluación continua de la aplicabilidad y relevancia de los tratados y convenios existentes en el contexto digital en constante evolución. Esto implica considerar los avances tecnológicos, los nuevos desafíos y las mejores prácticas en términos de seguridad, privacidad y protección de datos. Además, se deben explorar mecanismos de cooperación y diálogo entre los Estados para abordar las lagunas y desafíos del ciberespacio de manera efectiva.

La Convención de Viena sobre Relaciones Diplomáticas puede ser aplicada en el ciberespacio en relación con las violaciones de sistemas informáticos pertenecientes a misiones diplomáticas. Sin embargo, se requiere una adaptación del tratado para abordar específicamente los desafíos del ciberespacio, como establecer pautas y normas claras sobre el uso seguro de las tecnologías de la información y la comunicación en las sedes diplomáticas.

Además de estos tratados, existen otros instrumentos legales y marcos normativos relevantes para el ciberespacio, como:

La Carta de las Naciones Unidas: Proporciona un marco general para el mantenimiento de la paz y la seguridad internacionales, y puede ser aplicada en el contexto de ciberataques que amenacen la paz y seguridad internacionales.

El Grupo de Expertos Gubernamentales sobre el Ciberespacio de las Naciones Unidas: Establecido para examinar cuestiones relacionadas con la seguridad en el ciberespacio, ha producido varios informes que ofrecen orientación sobre cómo aplicar el derecho internacional existente en el ámbito digital.

Es importante tener en cuenta que el ciberespacio presenta desafíos únicos y en constante evolución, lo que requiere una adaptación constante del derecho internacional existente. Los Estados y las organizaciones internacionales continúan discutiendo y trabajando en la elaboración de normas y principios específicos para abordar los desafíos del ciberespacio de manera efectiva.

Propuesta de nuevas normas y tratados ante las insuficiencias del derecho internacional vigente

La elaboración de nuevos tratados y normas requiere un proceso de negociación y consenso entre los Estados. El ciberespacio es un entorno dinámico y en constante evolución, por lo que cualquier marco regulatorio debe ser flexible y adaptarse a los cambios tecnológicos y sociales. Por lo que, desde la visión del autor de esta investigación, es sumamente complejo realizar una propuesta de normas ante las insuficiencias del derecho internacional vigente, sin embargo, es posible apuntar hacia lo siguiente: **Proponer (**Consejo de Europa, 1981; Comisión Europea, 2016; DeNardis, 2014; Naciones Unidas, 2013; Schmitt, & Vihul, 2019)**:**

Tratado Internacional de Protección de Datos

Un tratado que establezca estándares internacionales para la protección de datos personales en línea. Podría incluir principios como el consentimiento informado, la minimización de datos, la seguridad de la información y los derechos de los individuos sobre sus datos.

Convención Internacional sobre Privacidad en Línea

Un tratado que garantice la protección de la privacidad en línea de los individuos, estableciendo límites claros sobre la recopilación, uso y divulgación de información personal en el ciberespacio. También podría abordar aspectos como la transparencia, el derecho al olvido y la protección de datos sensibles.

Convención sobre Responsabilidad de los Estados en el Ciberespacio

Un tratado que establezca las responsabilidades de los Estados en relación con los ciberataques y la ciberseguridad. Podría abordar temas como la no participación en ataques cibernéticos, la cooperación internacional en la investigación y atribución de ataques, y la asistencia a las víctimas de ciberataques.

Declaración Internacional de Derechos Humanos en el Ciberespacio

Una declaración que reafirme la aplicabilidad de los derechos humanos existentes en el entorno digital y establezca principios específicos para proteger y promover los derechos en línea. Podría incluir aspectos como la libertad de expresión, la privacidad, la no discriminación y el acceso a Internet como un derecho fundamental.

Privacidad en línea y protección de datos

Es crucial establecer normas internacionales que protejan la privacidad en línea y regulen la recopilación, uso y transferencia de datos personales. Estas normas podrían basarse en el Reglamento General de Protección de Datos de la Unión Europea (GDPR) y en el Convenio 108 del Consejo de Europa sobre Protección de Datos. También se pueden considerar principios como el consentimiento informado, la minimización de datos y la rendición de cuentas en el contexto digital.

Responsabilidad de los Estados

Es necesario establecer normas claras sobre la responsabilidad de los Estados en relación con las actividades cibernéticas. Esto implica definir las obligaciones de los Estados para prevenir y responder a los ataques cibernéticos, así como para proteger la infraestructura crítica y garantizar la seguridad cibernética. El Manual de Tallin 2.0 sobre el Derecho Internacional Aplicable a las Operaciones Cibernéticas es una referencia relevante para el desarrollo de normas en este ámbito.

Protección de los derechos humanos en el entorno digital

Los derechos humanos deben ser protegidos y promovidos en el ciberespacio. Es necesario desarrollar normas internacionales que aborden cuestiones como la libertad de expresión, el acceso a la información, la libertad de asociación y la privacidad en línea. La Declaración Conjunta de Libertad de Expresión y Privacidad en el Ciberespacio, elaborada por relatores especiales de las Naciones Unidas, puede ser una referencia útil para el desarrollo de nuevas normas.

Es importante tener en cuenta que estas propuestas son solo ejemplos y que cualquier nuevo instrumento internacional debe ser el resultado de un proceso inclusivo y consultivo que involucre a múltiples actores, incluidos los Estados, la sociedad civil y el sector privado.

Mecanismos de cooperación

Enfrentar los desafíos de la regulación del ciberespacio desde el derecho internacional requiere del fortalecimiento de la cooperación internacional promoviendo el intercambio de información, la asistencia técnica y el desarrollo de capacidades en materia de ciberseguridad, para lo que se pudieran activar los mecanismos de cooperación siguientes (Organización de los Estados Americanos (OEA), 2017, Human Rights Watch, 2017).

Foros y plataformas de diálogo multilateral

Se pueden establecer foros internacionales sobre ciberseguridad donde los Estados, organizaciones internacionales y actores relevantes puedan discutir y compartir mejores prácticas, desafíos y soluciones en el ámbito de la regulación del ciberespacio. Un ejemplo de esto es la Conferencia Internacional de Seguridad Cibernética, organizada por la Organización de las Naciones Unidas (ONU), que reúne a expertos en ciberseguridad de todo el mundo para intercambiar conocimientos y experiencias.

Acuerdos bilaterales y regionales

Los Estados pueden establecer acuerdos bilaterales y regionales para promover la cooperación en materia de ciberseguridad y el intercambio de información. Estos acuerdos pueden incluir disposiciones sobre el intercambio de datos, la asistencia mutua en investigaciones cibernéticas y el desarrollo conjunto de capacidades. Un ejemplo es el Acuerdo de Asistencia Mutua en Ciberseguridad de la Organización de los Estados Americanos (OEA), que busca fortalecer la cooperación en esta área en el continente americano.

Programas de asistencia técnica y desarrollo de capacidades

Los Estados y las organizaciones internacionales pueden proporcionar asistencia técnica y apoyo en el desarrollo de capacidades en materia de ciberseguridad a los países que lo necesiten. Esto puede incluir la capacitación de personal, la creación de centros de respuesta a incidentes cibernéticos y el fortalecimiento de la legislación y marcos normativos nacionales. La Iniciativa de Ciberseguridad de la Unión Europea (EU Cybersecurity Initiative) es un ejemplo de un programa integral que ofrece asistencia técnica y financiera a los Estados miembros de la Unión Europea para mejorar su capacidad de ciberseguridad.

Compartir información y buenas prácticas

Los Estados y las organizaciones internacionales pueden promover el intercambio de información y buenas prácticas en el ámbito de la ciberseguridad. Esto puede incluir la creación de plataformas seguras para compartir información sobre amenazas cibernéticas, la colaboración en la identificación y mitigación de vulnerabilidades, y el establecimiento de estándares comunes de seguridad. La Alianza Internacional de la Seguridad Cibernética (ICSA, por sus siglas en inglés) es un ejemplo de iniciativa para facilitar el intercambio de información y la colaboración entre los actores de la industria de la ciberseguridad.

Establecimiento de Redes de Puntos de Contacto Nacionales

Cada país podría designar un punto de contacto nacional responsable de facilitar la cooperación y el intercambio de información en materia de ciberseguridad. Estas redes de puntos de contacto podrían coordinarse a nivel regional e internacional para mejorar la colaboración en la respuesta a incidentes y compartir conocimientos técnicos.

Establecimiento de Normas y Principios Comunes

Los Estados podrían trabajar en la elaboración de normas y principios comunes en materia de ciberseguridad, privacidad y protección de datos. Esto ayudaría a crear un marco global coherente y facilitaría la cooperación internacional en la regulación del ciberespacio.

Promoción de la confianza y la transparencia entre los actores del ciberespacio

La creación de un Marco Internacional para la Confianza y Transparencia en el Ciberespacio promueve la confianza mutua y la transparencia entre los actores del ciberespacio, permitiendo reducir los conflictos y las tensiones en este ámbito y facilitando la cooperación internacional (Paris Call for Trust and Security in Cyberspace, 2018). Para lograrlo, es necesario establecer normas de comportamiento responsable,

promover la divulgación de vulnerabilidades y garantizar la rendición de cuentas por las acciones en línea. La implementación de este marco requiere de la cooperación de todos los actores involucrados, siendo fundamental un enfoque colaborativo y multistakeholder.

Con el fin de fomentar la confianza mutua y la transparencia entre los actores del ciberespacio, proponemos la creación de un Marco Internacional para la Confianza y Transparencia en el Ciberespacio. Esta iniciativa se basa en la adopción de normas de comportamiento responsable, la divulgación de vulnerabilidades y la rendición de cuentas por las acciones en línea, con el objetivo de reducir los conflictos y las tensiones en el ciberespacio y facilitar la cooperación internacional (United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (2015).

Normas de comportamiento responsable

Para fomentar la confianza mutua, es esencial establecer normas de comportamiento responsable en el ciberespacio. Estas normas deben abordar aspectos como el respeto a los derechos humanos, la protección de datos personales, la privacidad en línea y la responsabilidad en la difusión de información. Además, se deben promover principios de igualdad, no discriminación y respeto a la diversidad de opiniones. Esta propuesta se inspira en el Acuerdo de París y la Convención de Ginebra, que establecen estándares internacionales para abordar cuestiones globales (Muñoz, & Maró, 2020).

Divulgación de vulnerabilidades

La divulgación de vulnerabilidades es otro aspecto fundamental para fomentar la confianza y transparencia en el ciberespacio. Los actores del ciberespacio deben estar comprometidos a compartir información sobre vulnerabilidades descubiertas en sistemas de tecnología de la información y comunicación (TIC) de manera responsable y coordinada (Ponemon Institute, 2021). Esto permitirá que los afectados tomen las medidas necesarias para protegerse y mejorar la seguridad de sus sistemas. Para fortalecer este proceso, se deben establecer mecanismos de comunicación seguros y confiables, así como incentivos para motivar la divulgación responsable.

Rendición de cuentas por las acciones en línea

La rendición de cuentas por las acciones en línea es un elemento clave para fomentar la confianza y la transparencia en el ciberespacio. Los actores del ciberespacio deben asumir la responsabilidad de sus acciones digitales, especialmente en casos de ataques cibernéticos, propagación de información falsa y actividades ilegales en línea. Esto implica la colaboración entre gobiernos, organizaciones internacionales, sector privado y sociedad civil para garantizar que los responsables sean identificados y enfrenten las consecuencias legales correspondientes.

Cooperación internacional

La creación de este Marco Internacional para la Confianza y Transparencia en el Ciberespacio requiere de una cooperación internacional sólida. Los Estados, organizaciones internacionales, sector privado y sociedad civil deben trabajar de manera conjunta para establecer estándares globales, compartir buenas prácticas y promover la adhesión a este marco. Además, se deben establecer mecanismos de cooperación técnica y asistencia mutua para garantizar una implementación efectiva y una respuesta coordinada frente a los desafíos del ciberespacio.

Salvaguardia de los derechos humanos en línea

Educación en derechos humanos digitales

Es fundamental brindar educación sobre los derechos humanos en el ciberespacio para crear conciencia sobre la importancia de protegerlos. Esto incluye la promoción de la alfabetización digital y el fomento de habilidades para utilizar de manera segura y responsable la tecnología.

Desarrollo de leyes y políticas claras

Es necesario establecer leyes y políticas que protejan los derechos humanos en el ciberespacio y que sean claras en términos de sus aplicaciones y sanciones. Estas deben estar basadas en principios como la libertad de expresión, la privacidad y el acceso a la información.

Colaboración público-privada

La cooperación entre gobiernos, empresas y sociedad civil es fundamental para promover la protección de los derechos humanos en línea. Esto implica la adopción de estándares y prácticas conjuntas que respeten los derechos fundamentales en el ciberespacio.

Protección de la privacidad

Es necesario fortalecer las regulaciones y medidas de seguridad que protejan la privacidad de los usuarios en línea. Esto incluye el cifrado de datos, la protección de la identidad en línea y la limitación del acceso indebido a la información personal.

Fomento de la libertad de expresión

Es importante garantizar que todas las personas tengan la libertad de expresarse en el ciberespacio sin temor a represalias. Esto implica promover la diversidad de opiniones y evitar la censura y la vigilancia excesiva.

Transparencia y rendición de cuentas

Es fundamental que tanto los gobiernos como las empresas rindan cuentas por sus acciones en el ciberespacio. Esto implica la publicación de informes de transparencia que muestren cómo se maneja la información personal y cómo se protegen los derechos de los usuarios.

Fortalecimiento de la ciberseguridad

La ciberseguridad es un desafío urgente en el mundo actual, y es necesario adoptar medidas técnicas y legales para prevenir y responder de manera efectiva a los ataques cibernéticos. La promoción de estándares de seguridad, la capacitación de profesionales en ciberseguridad y la cooperación internacional son elementos clave en esta propuesta de fortalecimiento de la ciberseguridad. Esta propuesta tiene como objetivo fortalecer la ciberseguridad mediante la promoción de estándares de seguridad, la capacitación de profesionales en ciberseguridad y la cooperación en la detección y mitigación de amenazas.

Promoción de estándares de seguridad

Es necesario promover la implementación de estándares de seguridad reconocidos internacionalmente, como el ISO 27001, que proporciona un marco de gestión de seguridad de la información. Se deben establecer políticas y procedimientos para garantizar la protección de la información y la infraestructura tecnológica, así como para asegurar la continuidad del negocio en caso de un incidente cibernético.

Implementación de medidas de seguridad en infraestructuras críticas

Las infraestructuras críticas, como el sector energético, las comunicaciones y la banca, deben contar con medidas de seguridad adecuadas para protegerse de posibles ataques cibernéticos. Se deben implementar mecanismos de detección y prevención de intrusiones, así como sistemas de respaldo y recuperación de datos.

Actualización de la legislación en materia de ciberseguridad

Es necesario adecuar la legislación existente a los nuevos desafíos en el ámbito de la ciberseguridad. Se deben establecer sanciones proporcionales y efectivas para los perpetradores de ataques cibernéticos.

Cooperación internacional en la lucha contra los ataques cibernéticos

Se debe fomentar la cooperación entre países para intercambiar información y mejores prácticas en la detección y mitigación de amenazas cibernéticas. Se deben establecer acuerdos de cooperación en el ámbito de la ciberseguridad para facilitar la investigación y enjuiciamiento de los perpetradores de los ataques cibernéticos.

Capacitación

Formación y capacitación de profesionales en ciberseguridad

Es necesario promover la formación y capacitación de profesionales en ciberseguridad para mejorar las habilidades y conocimientos necesarios para prevenir y responder a los ataques cibernéticos. Se deben establecer programas educativos especializados en ciberseguridad y promover la certificación de profesionales en el campo.

Creación de centros de excelencia en ciberseguridad

Se deben establecer centros de excelencia en ciberseguridad que sirvan como plataformas de investigación y desarrollo de nuevas tecnologías y estrategias de ciberseguridad. Estos centros pueden colaborar con el sector público y privado en la detección y mitigación de amenazas cibernéticas.

Conclusiones

El ciberespacio representa un ámbito transnacional en el que se llevan a cabo muchas actividades, como el comercio electrónico, la comunicación, el acceso a la información y la transferencia de datos. Sin embargo, también se ha convertido en un terreno propicio para la comisión de delitos, como el robo de información, la piratería informática y los ataques cibernéticos.

El derecho internacional es el sistema de normas y principios que rigen las relaciones entre los Estados, pero también se aplica a otros actores internacionales, como las organizaciones internacionales y las empresas multinacionales. En el contexto del ciberespacio, el derecho internacional desempeña un papel fundamental para establecer límites y regular las conductas de los actores involucrados.

Uno de los desafíos para la aplicación efectiva del derecho internacional en el ciberespacio es la falta de consenso sobre cómo se aplican las normas y principios existentes a las actividades en línea. Además, la naturaleza transnacional del ciberespacio dificulta la identificación y persecución de los responsables de los delitos cibernéticos, ya que estos pueden operar desde cualquier lugar del mundo.

Para abordar estos desafíos, es fundamental fortalecer la cooperación internacional en la lucha contra los delitos cibernéticos. Esto implica la creación y fortalecimiento de mecanismos de cooperación entre los Estados, así como la promoción de la colaboración entre los sectores público y privado. Además, es necesario fomentar la capacitación y el intercambio de conocimientos sobre ciberseguridad y derecho internacional, para mejorar la comprensión y aplicación de las normas y principios existentes.

Asimismo, es importante promover la adopción de normas internacionales claras y consistentes sobre ciberseguridad y protección de datos. Esto proporcionaría un marco común para la regulación de las conductas en línea y facilitaría la identificación y persecución de los responsables de los delitos cibernéticos.

Referencias bibliográficas

Alianza Internacional de la Seguridad Cibernética (ICSA, por sus siglas en inglés). (s.f.). https://www.icsalliance.org/

Brownlie, I. (2008). *Principles of Public International Law* (7th ed.). Oxford University Press.

Cadwalladr, C. (2018). The Cambridge Analytica Files: 'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Cisco. (2021). Cisco Annual Cybersecurity Report 2021. https://www.cisco.com/c/en/us/products/security/security-reports.html

Comisión Europea. (2016). Reglamento General de Protección de Datos (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Consejo de Europa. (1981). Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108). https://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/108

Consejo de Europa. (2004). Convención sobre Cibercrimen (Convención de Budapest). https://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/185

DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.

Dinstein, Y. (2018). *War, Aggression and Self-Defense* (6th ed.). Cambridge University Press.

DiResta, R., & Shaffer, J. (2018). The Tactics & Tropes of the Internet Research Agency. https://www.newknowledge.com/disinforeportjan2019

Goldsmith, J. L., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press.

Human Rights Watch. (2017). Internet Freedom. https://www.hrw.org/es/internet-freedom

Kshetri, N. (2017). Global Entrepreneurship and Development Index 2017. Springer.
Muñoz, L., & Maró, A. (2020). *Ciberseguridad: guía para directivos*. Instituto Nacional de Ciberseguridad (España).
Naciones Unidas. (1961). Convención de Viena sobre Relaciones Diplomáticas. https://www.un.org/es/documents/treaty/files/convencion_viena.pdf
Naciones Unidas. (2013). Declaración Conjunta de Libertad de Expresión y Privacidad en el Ciberespacio. https://www.ohchr.org/SP/Issues/FreedomOpinion/Pages/DigitalAge.aspx
Organización de los Estados Americanos (OEA). (2017). Acuerdo de Asistencia Mutua en Ciberseguridad. http://www.oas.org/juridico/spanish/cyb_acuerdo_ciberseguridad.pdf.
Ponemon Institute. (2021). Cost of Cyber Crime Study: Global Analysis. https://www.accenture.com/us-en/insights/security/cost-of-cyber-crime-study
Rosenzweig, P., & Nakatani, P. (2017). International Cybersecurity Law. Oxford University Press.
Schmitt, M. N., & Vihul, L. (eds.). (2019). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
UN General Assembly. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. https://undocs.org/A/70/174.
United Nations Office on Drugs and Crime. (2001). Convention on Cybercrime (Budapest Convention). https://www.unodc.org/cybercrime/es/cybercrimeconvention.html
US Department of Justice. (2021). Colonial Pipeline Company and Affiliates to Pay $154 Million in Penalties to Resolve Allegations of Violating the Clean Air Act and Spill Prevention, Control, and Countermeasure Regulations. https://www.justice.gov/opa/pr/colonial-pipeline-company-and-affiliates-pay-154-million-penalties-resolve-allegations.