DERECHO INTERNACIONAL Y CIBERSEGURIDAD: DESAFÍOS Y OPORTUNIDADES

INTERNATIONAL LAW AND CYBERSECURITY: CHALLENGES AND OPPORTUNITIES

Maykel Ponçoni[1]

Universidade Presbiteriana Mackenzie

Cómo citar:

Ponçoni, M. (2024). Derecho internacional y ciberseguridad: desafíos y oportunidades. *Memorias II Congreso Internacional de Gobierno y Relaciones Internacionales "Solidaridad, paz y seguridad internacional"*. Universidad La Gran Colombia.

Resumen

El artículo analiza los desafíos legales de la ciberseguridad en el ámbito internacional, destacando su relevancia en un mundo cada vez más dependiente de tecnologías digitales. Señala que la vulnerabilidad a ciberataques amenaza la seguridad nacional e internacional, lo que requiere una cooperación entre estados para mitigar los riesgos. El estudio evalúa la efectividad de los marcos legales y tratados internacionales vigentes, como el Convenio de Budapest, y explora oportunidades para fortalecer estándares globales mediante prácticas colaborativas. Metodológicamente, se basa en un enfoque bibliográfico y documental, revisando fuentes académicas (artículos, tesis, legislación) de bases de datos especializadas en derecho y ciberseguridad. El análisis crítico de estas fuentes identifica vacíos en la regulación actual, como la falta de mecanismos vinculantes para la aplicación de normas, y propone mejoras en coordinación interestatal. Concluye que, aunque existen avances en normativas, la dinámica cambiante de las amenazas cibernéticas exige marcos

[1] Doctora y magíster en Derecho Político y Económico por la Universidade Presbiteriana Mackenzie (Brasil), doctora en Ciencias Jurídicas y Sociales por la Universidad del Museo Social Argentino (Argentina), especialista en Derecho Público por la Universidade Gama Filho (Brasil), licenciada en Derecho por la Universidad de Cuiabá (Brasil) y licenciada en Enfermería por la Universidad Federal de Mato Grosso (Brasil). Empleada publica del Gobierno del Estado de Mato Grosso que actúa en la Contraloría General, en el área de corrección. Correo electrónico: maykel.pon@gmail.com. Linkedin: https://n9.cl/8ph99o

más flexibles y adaptativos, respaldados por una cooperación técnica y política sólida entre países. El texto subraya la necesidad de equilibrar soberanía nacional con responsabilidad global para garantizar seguridad digital, enfatizando el rol de instituciones internacionales en facilitar diálogos multilaterales.

Palabras clave: ciberseguridad, cooperación internacional, marcos legales internacionales, vulnerabilidad digital.

Abstract

The article analyses the legal challenges of cybersecurity in the international arena, highlighting its relevance in a world increasingly dependent on digital technologies. It points out that vulnerability to cyberattacks threatens national and international security, requiring cooperation between states to mitigate risks. The study evaluates the effectiveness of current legal frameworks and international treaties, such as the Budapest Convention, and explores opportunities to strengthen global standards through collaborative practices. Methodologically, it is based on a bibliographic and documentary approach, reviewing academic sources (articles, theses, legislation) from specialized databases on law and cybersecurity. The critical analysis of these sources identifies gaps in current regulation, such as the lack of binding mechanisms for the application of standards and propose improvements in interstate coordination. It concludes that, although there are advances in regulations, the changing dynamics of cyber threats require more flexible and adaptive frameworks, supported by solid technical and political cooperation between countries. The text underlines the need to balance national sovereignty with global responsibility to ensure digital security, emphasizing the role of international institutions in facilitating multilateral dialogues.

Keywords: cybersecurity, international cooperation, international legal frameworks, digital vulnerability.

Introducción

En el mundo interconectado de la actualidad, las tecnologías digitales se han consolidado como una fuerza transformadora en varios sectores, y el sector público no es una excepción. La ciberseguridad se ha convertido en una preocupación central para estados, organizaciones e individuos. La creciente dependencia de los sistemas digitales y las redes de información ha aumentado la vulnerabilidad a los ciberataques, que pueden tener consecuencias devastadoras para la seguridad nacional e internacional.

Este artículo busca explorar los desafíos legales que surgen de la ciberseguridad en el contexto internacional y examinar cómo la cooperación entre Estados puede contribuir a la seguridad global. El análisis abordará la efectividad de los marcos legales y tratados internacionales actuales, así como las oportunidades para el desarrollo de nuevos estándares y prácticas colaborativas.

Para la realización de esta investigación, se adoptó un enfoque metodológico de carácter bibliográfico y documental, con énfasis en el análisis de la legislación y tratados internacionales relevantes en materia de ciberseguridad. La investigación comenzó con la selección de fuentes académicas, artículos científicos, tesis y disertaciones, disponibles en bases de datos y revistas específicas del área de Derecho y Ciberseguridad. Los materiales seleccionados son analizados críticamente, destacando las principales teorías, conceptos y discusiones sobre el tema.

Esta metodología permite una comprensión crítica del panorama jurídico actual relacionado con la ciberseguridad, así como de las posibilidades de mejora y cooperación internacional.

Desafíos legales en ciberseguridad

Los avances de la tecnología actual, que comenzaron con la creación de computadoras y su interoperatividad en red, permitieron compartir datos, reduciendo las distancias físicas. "El mundo se ha vuelto más integrado y el planeta se ha transformado en una aldea global" (Nunes, 2010). Por tanto, esta facilidad de acceso a la información y a los sistemas trajo nuevos riesgos relacionados con la exposición virtual.

La ciberseguridad es un concepto multifacético y no existe un consenso global sobre su definición. Según ISO/IEC 27032:2012, la ciberseguridad implica preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. La Unión Europea adopta una visión más integral, definiéndola como las actividades necesarias para proteger las redes, los sistemas de información, sus usuarios y otras personas afectadas por las ciberamenazas. En el Reino Unido, la definición se centra en proteger los sistemas interconectados (*hardware*, *software* e infraestructura), datos y servicios contra el acceso no autorizado y el uso indebido, incluidos los daños causados por operadores intencionales o accidentales. Colombia destaca la ciberseguridad como una capacidad del Estado para minimizar los riesgos a los ciudadanos y proteger los bienes del Estado, abarcando recursos, políticas, lineamientos y métodos de gestión de riesgos. Esta definición colombiana enfatiza el papel central del Estado en la provisión de ciberseguridad (Hurel, 2021).

Definición de ciberataques en el Derecho Internacional

Los ciberataques son una preocupación creciente en el Derecho Internacional, dada su capacidad de trascender fronteras y causar daños importantes a infraestructuras

críticas, tanto públicas como privadas, esto que trae consigo importantes desafíos relacionados con la seguridad y la privacidad.

Un ciberataque puede entenderse como cualquier intento de comprometer la confidencialidad, integridad y disponibilidad de datos o sistemas tecnológicos. También destaca que los ciberataques tienen como objetivo causar daños u obtener control o acceso a documentos y sistemas importantes en una red informática personal o comercial. Estos ataques son llevados a cabo por individuos u organizaciones con intenciones políticas, criminales o personales de destruir o acceder a información confidencial, según el sitio web de Microsoft (s.f.).

La clasificación de estos ataques involucra varios aspectos como considerar la intención del agente, los métodos utilizados y los efectos producidos. Estas variables son complejas y dinámicas, lo que dificulta formular una definición integral que sea universalmente aceptada. Además, las tecnologías y técnicas de ataque que evolucionan rápidamente añaden una capa adicional de complejidad (Borges, 2018).

En los delitos cibernéticos hay dos sujetos: el *hacker* y el *cracker*. Comúnmente, la palabra *hacker* se relaciona con delitos virtuales, pero los verdaderos delincuentes son los *crackers*. La distinción entre estas dos figuras radica en la forma en que utilizan el conocimiento tecnológico. Mientras que los primeros son programadores con grandes conocimientos sobre tecnología e internet, y carentes de intenciones delictivas, los *crackers*

> […] derivan del verbo inglés “*to crack*”, que significa romper. Entre las acciones se encuentran la práctica de violar sistemas de seguridad, códigos de encriptación y contraseñas de acceso a redes, de manera ilegal y con intención de invadir y sabotear con fines delictivos. (Cassanti, 2018)

El Derecho Internacional enfrenta dificultades para aplicar sus principios tradicionales al ciberespacio debido a su naturaleza fluida y la ausencia de una autoridad centralizada. La jurisdicción y atribución de los delitos cibernéticos a determinados países o individuos representan cuestiones complejas y ambiguas, que requieren una reformulación de los sistemas educativos y legales para adaptarse mejor a las nuevas realidades digitales (Branco y Talpai, 2023).

Problemas al clasificar diferentes tipos de ataques y su gravedad

Clasificar los ciberataques es un desafío importante en el campo de la seguridad digital y el derecho internacional. Determinar su gravedad es una tarea compleja e involucra varios factores, incluida la naturaleza del ataque, el objetivo del atacante, los métodos utilizados y las consecuencias del ataque.

La definición de ciberataque debe considerar aspectos como la intención del agente, los métodos utilizados y los efectos del ataque. Sin embargo, estas variables son complejas y dinámicas, lo que dificulta formular una definición integral que sea universalmente aceptada. La rápida evolución de las tecnologías y técnicas de ciberataque añade una capa adicional de complejidad (Bortot, 2017). La gravedad es mayor cuando el ataque se lleva a cabo utilizando técnicas avanzadas que pueden burlar medidas de seguridad sólidas (Datasafer, 2024).

Los diferentes tipos de ataques, como *malware*, *phishing*, ataques de denegación de servicio e intrusiones en el sistema, tienen diferentes características y niveles de gravedad. Establecer una clasificación estandarizada que permita

evaluar adecuadamente la gravedad de cada ataque es crucial para formular respuestas jurídicas proporcionales y efectivas (Nunes, 2015).

Los ataques cibernéticos pueden tener diversos objetivos, incluyendo el robo de datos, el vandalismo digital, el espionaje corporativo o gubernamental, e incluso el ciberterrorismo. La intención detrás de cada ataque es un elemento fundamental para determinar su gravedad.

La gravedad de un ataque también se puede evaluar en función del objetivo. Los ataques a infraestructuras críticas, como redes eléctricas, sistemas de salud o datos gubernamentales, generalmente se consideran más graves debido a sus consecuencias potencialmente catastróficas (Datasafer, 2024).

En el contexto del Derecho Internacional, la falta de consenso sobre los criterios de clasificación y gravedad de los ciberataques dificulta la armonización de la legislación y la cooperación entre estados (Nunes, 2015).

Desafíos adicionales

Además de las dificultades de definición y clasificación, existen otros desafíos legales importantes en ciberseguridad relacionados con la jurisdicción y la soberanía.

Jurisdicción: determinar la jurisdicción adecuada para hacer frente a los ciberataques es complejo, dada la naturaleza transnacional de la mayoría de estos ataques. La ausencia de fronteras físicas en el ciberespacio dificulta identificar el origen de los ataques y, en consecuencia, el sistema jurídico competente para juzgar a los responsables (Silva, 2020).

Evidencia: recopilar y preservar evidencia digital presenta desafíos únicos, incluida la volatilidad de los datos digitales y la dificultad de autenticar la evidencia. Sin una base probatoria sólida, responsabilizar a los perpetradores de ciberataques se vuelve aún más complicado (Oliveira, 2019).

Derechos humanos y privacidad: las medidas de ciberseguridad, incluida la vigilancia y el seguimiento, deben equilibrar los derechos humanos y la privacidad de las personas. La formulación de políticas que garanticen la seguridad sin comprometer las libertades individuales es un desafío constante (Santos, 2017).

Soberanía y jurisdicción

La guerra tradicional se basa en el territorio y la soberanía, lo que establece fronteras claras y jurisdicción definida. Sin embargo, en el contexto de la ciberguerra, estes límites se vuelven indefinidos, lo que dificulta la aplicación de las normas tradicionales de soberanía de cada Estado en el ciberespacio. La naturaleza global y descentralizada del ciberespacio plantea desafíos importantes a la soberanía estatal y al Derecho Internacional, y requiere nuevas metodologías para garantizar la paz mundial y la seguridad internacional.

Como lo analizan Fonseca y Rodrigues (2024), la soberanía y la condición de Estado en el ciberespacio requieren nuevas fronteras y desafíos para enfrentarse de manera efectiva. Las interacciones globales facilitadas por Internet amplían las posibilidades de daño, lo que requiere que los Estados reconsideren sus enfoques tradicionales de jurisdicción y regulación.

La definición de delito cibernético de la Organización para la Cooperación y el Desarrollo Económico (OCDE) se describe como “cualquier comportamiento

ilegal, poco ético o no autorizado que implique el procesamiento automático de datos y/o la transmisión de datos” (OCDE, 2016).

La ciberguerra fue definida según Richard A. Clarke y Robert K. Knake (2010) de la siguiente manera:

> Es la penetración no autorizada, en nombre o apoyo de un gobierno de otra nación, computadora o red, o cualquier otra actividad que afecte un sistema informático, en el que el objetivo es agregar, alterar o falsificar datos o causar interrupción o daño a una computadora, un dispositivo de red o los objetos de los controles del sistema informático. (p. 228, traducción propia)

Para hacer frente a estos desafíos, la autorregulación, el arbitraje y la mediación pueden surgir como alternativas viables para resolver conflictos en el ciberespacio, como sugiere Atheniense (2002). Estos enfoques alternativos son cruciales para equilibrar la necesidad de proteger los derechos de los ciudadanos y respetar la naturaleza global y sin fronteras de Internet.

La aplicación del Derecho Internacional en el ciberespacio es un área en desarrollo, con esfuerzos continuos por parte de organizaciones como la OTAN y las Naciones Unidas para establecer protocolos regulatorios y de cooperación apropiados. Sin embargo, persisten lagunas importantes, especialmente a la hora de determinar la jurisdicción de los delitos cibernéticos y asignar responsabilidades, debido a la naturaleza anónima y transfronteriza de Internet (Atheniense, 2002).

Cuestiones de soberanía en relación con las actividades cibernéticas que cruzan fronteras

La soberanía estatal es un principio fundamental del derecho internacional, que se basa en la autoridad exclusiva de un Estado sobre su territorio y sus asuntos

internos. Sin embargo, en el contexto de las actividades cibernéticas, este concepto enfrenta importantes desafíos. La naturaleza transnacional de Internet y los ciberataques complica la aplicación de los principios tradicionales de soberanía.

Un ciberataque puede, por ejemplo, originarse en un país y causar daños sustanciales en otro, sin que exista una violación física de las fronteras. Esto plantea interrogantes sobre hasta qué punto un Estado puede ejercer su soberanía para defenderse de tales ataques y perseguir a los responsables (Carvalho, 2015).

Además, la cibersoberanía implica la capacidad de los Estados de regular el uso de Internet dentro de sus fronteras, lo que puede generar conflictos con otros Estados que tienen normas y enfoques diferentes hacia el ciberespacio. La falta de un consenso global sobre las normas y principios que deben regir la cibersoberanía da como resultado una fragmentación jurídica que dificulta la cooperación internacional (Silva, 2017).

Desafíos en la aplicación de leyes nacionales a los delitos cibernéticos cometidos internacionalmente

Los delitos cibernéticos suelen involucrar a actores y víctimas ubicados en diferentes países, lo que complica la aplicación de las leyes nacionales. La jurisdicción extraterritorial, donde un Estado intenta aplicar sus leyes más allá de sus fronteras, es un concepto complejo y controvertido en el Derecho Internacional (Carvalho, 2015).

En primer lugar, identificar a los autores de los ciberataques es una tarea difícil debido a la posibilidad de mantener el anonimato y al uso de técnicas avanzadas de ocultación. Incluso cuando se identifica a los perpetradores, la falta

de acuerdos de extradición o la resistencia de los Estados a colaborar pueden impedir la responsabilidad legal (Costa & Silva, 2016).

En segundo lugar, la diversidad de legislaciones nacionales en materia de delitos cibernéticos crea un escenario en el que actos considerados ilegales en un país pueden no serlo en otro. Esto no sólo obstaculiza la aplicación de la ley, sino también la cooperación jurídica internacional. La ausencia de normas homogéneas significa que los ciberdelincuentes pueden aprovechar estas lagunas legales para evitar la captura y el castigo (Santos, 2013).

La necesidad de armonizar la legislación nacional para abordar el ciberdelito transnacional

Para abordar eficazmente el delito cibernético, es imperativo que los Estados trabajen para armonizar su legislación nacional. Esto no solo facilita la cooperación internacional, sino que también crea un entorno legal más predecible y consistente (Costa & Silva, 2016).

La armonización puede lograrse mediante la adopción de tratados y convenios internacionales que establezcan normas comunes para combatir el delito cibernético. El Convenio de Budapest sobre la ciberdelincuencia es un ejemplo notable, que proporciona un marco jurídico integral para la cooperación internacional y la armonización de las leyes nacionales. Sin embargo, no todos los países son signatarios de esta convención, lo que limita su efectividad global (Silva, 2017).

Además, es crucial la creación de mecanismos de cooperación internacional eficaces, como equipos conjuntos de investigación y plataformas para el

intercambio de información. La capacitación técnica y jurídica de los agentes encargados de hacer cumplir la ley y del poder judicial también es esencial para garantizar que puedan hacer frente a la complejidad de los delitos cibernéticos (Santos, 2013).

Finalmente, se necesita un fuerte compromiso político para abordar los desafíos de la soberanía y la jurisdicción en el ciberespacio. Esto implica no sólo la voluntad de adoptar e implementar estándares internacionales, sino también la voluntad de cooperar de manera transparente y efectiva con otros Estados (Mendonça, 2014).

Cooperación internacional en materia de ciberseguridad

La ciberseguridad requiere un enfoque colaborativo, siendo esencial para enfrentar las ciberamenazas, que no respetan fronteras y pueden causar daños importantes en múltiples países simultáneamente.

La interconexión de las infraestructuras digitales implica que la seguridad de un país frecuentemente depende de la seguridad de otros. Por lo tanto, la cooperación internacional puede mejorar la habilidad para prevenir, identificar y reaccionar ante incidentes cibernéticos.

El ciberespacio, debido a su naturaleza virtual, no está gestionado ni es propiedad de los gobiernos, sino de todos los usuarios de una sociedad de la información global. Debido al rápido desarrollo, el ciberespacio está en constante evolución y cambio. Por esta razón, los instrumentos clásicos de regulación y soberanía, establecidos por los Estados para reducir los riesgos que surgen del ciberespacio, son difíciles de implementar.

Al analizar las amenazas que surgen de la posibilidad de que actores hostiles exploten las vulnerabilidades de las infraestructuras de información de un país, debemos evaluar sus intenciones y capacidades para infligir daños a estas infraestructuras, con el fin de definir el nivel de amenaza a enfrentar. Las amenazas pueden materializarse a través de acciones llevadas a cabo por individuos aislados (aficionados, hackers o crackers), por grupos organizados (criminales, grupos de presión social o terroristas) o incluso por Estados (ciberguerra) (Nunes, 2012).

El intercambio de datos sobre amenazas, vulnerabilidades y mejores prácticas es fundamental para la cooperación internacional en ciberseguridad. La confianza entre los países es esencial para facilitar este intercambio y coordinar respuestas rápidas y efectivas a los incidentes cibernéticos, promoviendo una ciberseguridad más equitativa a nivel global.

Marcos legales internacionales

A lo largo de los años, varios países han intentado adaptar sus leyes para combatir el cibercrimen, con énfasis en Estados Unidos, primer país en legislar sobre el tema, y Europa, a través de la redacción de la Convención sobre el Cibercrimen, también conocida como Convención sobre la Ciberdelincuencia de Budapest, es uno de los principales instrumentos jurídicos internacionales en este campo, estableciendo normas para la penalización de conductas relacionadas con la ciberdelincuencia y promoviendo la cooperación entre los Estados signatarios (Consejo de Europa, 2001).

El Convenio de Budapest también proporciona un marco para la asistencia jurídica mutua, facilitando las investigaciones transnacionales y la aplicación de la

ley. Además de este Convenio, otros acuerdos e iniciativas internacionales han contribuido a la gobernanza de la ciberseguridad. Por ejemplo, las Naciones Unidas (ONU) han promovido debates sobre normas de comportamiento responsable en el ciberespacio, mientras que la Organización para la Cooperación y el Desarrollo Económico ha desarrollado directrices para la seguridad de las redes de información (OCDE, 2015).

En 1995, los organismos internacionales ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) dieron origen a un grupo de normas que consolidan los lineamientos relacionados con el alcance de la Seguridad de la Información, está representada por la serie 27000, 27002 (antiguo estándar 17799:2005), estándar internacional que establece un código de mejores prácticas para apoyar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones (ABNT, 2005).

Mientras tanto, en Brasil, el legislativo carece de insumos a la hora de esta lucha, lo que la hace favorable a los delincuentes.

La implementación eficaz de los marcos legales enfrenta numerosos desafíos, como las diferencias en las legislaciones nacionales, la rápida evolución de las amenazas cibernéticas y la necesidad de encontrar un equilibrio entre la seguridad y la protección de los derechos individuales y la privacidad. A pesar de estos desafíos, también se presentan oportunidades para mejorar la cooperación internacional y crear prácticas más efectivas en el ámbito de la ciberseguridad.

Desafíos de la cooperación internacional

A pesar de la importancia de la cooperación internacional, varios desafíos obstaculizan su implementación efectiva. Uno de los principales desafíos es la falta de consenso sobre las normas y principios que deben regir el ciberespacio.

Para superar estos desafíos y mejorar la cooperación internacional, se pueden considerar algunas medidas. En primer lugar, es necesario promover el diálogo y la construcción de confianza entre los Estados. Los foros internacionales, como las Naciones Unidas y el Foro Global sobre Ciberseguridad, pueden facilitar estos debates y ayudar a desarrollar estándares comunes (UN Secretary General & GGE, 2015).

En segundo lugar, es importante invertir en capacidades técnicas y jurídicas para mejorar la respuesta a los incidentes cibernéticos. La asistencia técnica y el desarrollo de capacidades pueden ayudar a los países con infraestructuras cibernéticas menos desarrolladas a fortalecer su ciberseguridad y participar más plenamente en la cooperación internacional (OCDE, 2015).

Finalmente, armonizar la legislación nacional en torno a estándares internacionales, como los establecidos por el Convenio de Budapest, puede facilitar la cooperación y la aplicación de la ley a nivel transnacional. La adopción de mecanismos de asistencia jurídica mutua y la creación de equipos conjuntos de investigación son pasos concretos que pueden mejorar la capacidad de los Estados para combatir el delito cibernético de manera colaborativa (Consejo de Europa, 2001).

La aplicación de la tecnología digital promete aumentar la eficiencia en la detección de actividades sospechosas, ofreciendo rapidez en los procesos. Sin

embargo, esta tecnología plantea desafíos, incluida la variabilidad y la calidad de los datos, y las cuestiones éticas y legales asociadas.

La importancia de la ratificación y la implementación uniforme de los acuerdos internacionales

La ratificación y la implementación uniforme de acuerdos internacionales sobre ciberseguridad desempeñan un papel crucial en la mitigación de las ciberamenazas a nivel global. A través de la cooperación internacional y la armonización de la legislación nacional, se promueve un entorno más seguro y confiable para todos los usuarios de las tecnologías de la información y la comunicación (TIC). La Convención de Budapest sobre ciberdelincuencia, adoptada en 2001 por el Consejo de Europa, es un ejemplo destacado de un tratado internacional que establece estándares comunes para la prevención, investigación y sanción de delitos informáticos. Sin embargo, la efectividad de estos acuerdos depende en gran medida de la ratificación y aplicación uniforme por parte de los Estados miembros (Council of Europe, 2001).

La Organización de las Naciones Unidas (ONU) también ha subrayado la importancia de la cooperación internacional en la protección contra amenazas cibernéticas a través de diversas resoluciones y recomendaciones. La Resolución 70/237 de la Asamblea General de la ONU, por ejemplo, insta a los Estados a fortalecer la seguridad de las TIC y a adoptar medidas para promover la confianza en el uso seguro de estas tecnologías (Naciones Unidas. Asamblea General, 2015).

La ratificación y aplicación uniforme de estos acuerdos internacionales no solo fortalece la respuesta colectiva frente a las amenazas cibernéticas, sino que

también facilita la cooperación transfronteriza en la investigación y enjuiciamiento de delitos informáticos. Es fundamental que los Estados se comprometan a cumplir con estos estándares internacionales para garantizar la efectividad de las medidas de ciberseguridad a nivel global.

El papel de las Naciones Unidas y otras organizaciones internacionales en la promoción de la ciberseguridad

Las Naciones Unidas han sido un actor clave en la promoción de la ciberseguridad a nivel global. La ONU ha facilitado la adopción de resoluciones y ha impulsado la creación de marcos jurídicos internacionales para enfrentar las amenazas cibernéticas. Uno de los principales esfuerzos en este sentido ha sido la adopción de la Resolución 64/211, que subraya la importancia de la cooperación internacional en materia de ciberseguridad (Naciones Unidas. Asamblea General, 2013).

Además, la ONU ha establecido el Grupo de Trabajo Abierto sobre la Seguridad en el Uso de las Tecnologías de la Información y las Comunicaciones, que busca desarrollar normas, reglas y principios de comportamiento responsable de los Estados en el ciberespacio.

La Organización de los Estados Americanos (OEA) también ha desempeñado un papel significativo en la promoción de la ciberseguridad en la región. La OEA ha implementado el Programa Interamericano de Ciberseguridad, que tiene como objetivo fortalecer las capacidades nacionales en materia de ciberseguridad y promover la cooperación entre los Estados miembros (Costa, 2014).

Uno de los logros importantes de la OEA ha sido la creación de equipos de respuesta a incidentes cibernéticos en varios países de América Latina, facilitando así una respuesta coordinada ante incidentes cibernéticos y promoviendo el intercambio de información y mejores prácticas (Oliveira, 2016).

La Unión Internacional de Telecomunicaciones (UIT), una agencia especializada de la ONU, ha sido fundamental en el desarrollo de estándares internacionales para la ciberseguridad. La UIT promueve la adopción de medidas de seguridad cibernética entre sus Estados miembros y ofrece asistencia técnica y formación para mejorar las capacidades nacionales.

El Programa Mundial de Ciberseguridad (GCA) de la UIT es un marco global que busca mejorar la cooperación internacional y proporcionar una estructura coherente para enfrentar las amenazas cibernéticas.

Conclusión

El avance tecnológico ha ofrecido grandes oportunidades, pero también ha expuesto vulnerabilidades ante ataques cibernéticos. Garantizar la ciberseguridad a nivel internacional requiere una estrategia que combine esfuerzos legislativos, diplomáticos y técnicos. La cooperación entre Estados, respaldada por un sólido marco jurídico, es clave para enfrentar estos desafíos. Es esencial definir claramente los ataques cibernéticos y establecer una clasificación estandarizada de su gravedad para crear un marco legal efectivo. La armonización de legislaciones y la formación técnica y jurídica son fundamentales para abordar las amenazas de manera coordinada.

En un entorno digital globalizado la cooperación internacional es fundamental para enfrentar los desafíos de la ciberseguridad. Aunque existen múltiples desafíos, como la falta de consenso en normas y la desconfianza entre Estados, también hay oportunidades significativas para mejorar la cooperación mediante el diálogo, la capacitación técnica y jurídica, y la armonización de legislaciones nacionales. El desarrollo de un marco jurídico internacional robusto y la promoción de una cultura de cooperación son cruciales para asegurar la ciberseguridad global.

Referencias

ABNT. (2005). *NBR ISO/IEC 27002 – Tecnología de la información – Técnicas de seguridad – Código de prácticas para la gestión de la seguridad de la información*. ABNT.

Agência Nacional de Telecomunicações. (2020). Políticas públicas. Agência Nacional de Telecomunicações. https://n9.cl/0jgjt2

Atheniense, A. (2002). A jurisdição no ciberespaço. https://bdjur.stj.jus.br/jspui/bitstream/2011/115040/1/jurisdicao_ciberespaco_atheniense.pdf

Lorenzo, J. V. (2002). A aplicação do direito internacional no ciberespaço: questões de soberania e jurisdição. *Revista FT*, *27*(122). https://10.5281/zenodo.7991598

Borges, J. P. (2018). Segurança cibernética e direito internacional: desafios e perspectivas. *Revista de Direito Internacional*. https://www.revistadireitointernacional.com.br

Bortot, J. F. (2017). Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas Legislações Brasileira e internacional. *VirtuaJus, 2*(2), 338-362. https://n9.cl/zzvmx3

Branco, P. G., & Talpai, B. (2023). A soberania e o ciberespaço: Uma análise crítica do conceito de soberania e globalização. *Juris. Revista da Faculdade de Dereito Brasil, 30*(1), 43-61. https://doi.org/10.14295/juris.v30i1.11285

Presidência da República Brasil. (2014, 23 de abril). Marco Civil da Internet. Lei Nº 12.965, de 23 de abril de 2014. https://n9.cl/e3bz8d

Carvalho, A. (2015). A soberania cibernética e a responsabilidade dos Estados no direito internacional. *Revista de Direito Internacional, 12*(1), 45-60. http://www.revistadireitointernacional.org/index.php/rdi/article/view/38

Cassanti, M. de O. (2014). *Crimes virtuais, vítimas reais* (1.ª ed.). Brasport.

Clarke, R. A., & Knake, R. K. (2010). *Cyberwar: The Next Threat to National Security and what to do about it*. Harper Collins.

Consejo de Europa. (2001). *Council of Europe Framework Convention on the Value of Cultural Heritage for Society*. https://n9.cl/7ip1k

Costa, P. R. (2014). La cooperación internacional en la ciberseguridad: el papel de la OEA. *Revista de Derecho Internacional, 11*(2), 130-145. http://www.revistas.uexternado.edu.co/index.php/derest/article/view/3805

Costa, P. R., & Silva, M. R. (2016). Jurisdição e competência no combate ao cibercrime: desafios e perspectivas. *Revista Brasileira de Direito, 12*(3), 58-75. https://seer.imed.edu.br/index.php/revistadedireito/article/view/1433

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention) ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Datasafer. (2024, 8 de enero). Retrospectiva: principais ataques cibernéticos de 2023. *Datasafer.* https://n9.cl/kz5r1

Fonseca, T. A. A. M., & Rodrigues, L. A. N. (2024). Soberania e estatalidade no ciberespaço: novas fronteiras, novos desafios. *Revista de Ciências do Estado, 9*(1), 1-5. https://periodicos.ufmg.br/index.php/revice/article/view/e53395

Hurel, L. M. (2021). Cibersegurança no Brasil: uma análise da estratégia nacional. *Artigo Estratégico* (54). Instituto Igarapé https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf

International Telecommunication Union. (2020). Global Cybersecurity Index (GCI) 2020. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Mendonça, S. A. (2014). Cibersegurança e a soberania dos Estados: uma análise crítica. *Revista Brasileira de Políticas Públicas, 5*(2), 123-139. https://rbpp.cespe.unb.br/index.php/RBPP/article/view/91

Microsoft. (s.f.). O que é um ataque cibernético? *Segurança da Microsoft*. https://n9.cl/u0yjv

Naciones Unidas. Asamblea General. (2014, 21 de enero). *Resolución 68/167: Seguridad en el uso de las tecnologías de la información y las comunicaciones*. Naciones Unidas https://undocs.org/es/A/RES/68/167

Naciones Unidas. Asamblea General. (2015). *Resolución 70/237. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*. Naciones Unidas. https://undocs.org/es/A/RES/70/237

Nunes, L. A. R. (2015). *Guerra cibernética e o direito internacional: aplicabilidade do jus ad bellum e do jus in bello* [trabajo de grado, Escola Superior de Guerra]. https://n9.cl/vot2ho

Nunes, L. A. R. (2010). *Guerra cibernética: está a MB preparada para enfrentá-la? Monografia* –[monografía, Escola de Guerra Naval]. https://n9.cl/aom4b

Nunes, P. F. V. (2012). A definição de uma estratégia nacional de cibersegurança. *Nação e Defesa*, (133-5), 113-127. https://revistas.rcaap.pt/nacao/article/download/38475/26558/172486

Organización para la Cooperación y el Desarrollo Económico [OCDE]. (2015). *Directrices de la OCDE para la seguridad de los sistemas de información y redes: hacia una cultura de seguridad*. OCDE. https://www.oecd.org/sti/ieconomy/15582260.pdf

Organisation for Economic Co-operation and Development [OECD]. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. OECD Publishing. https://acortar.link/ZguxgF

Organisation for Economic Co-operation and Development [OECD]. (2016). *Policy Framework on Digital Security: Cybersecurity for Prosperity*. OECD iLibrary. https://one.oecd.org/document/DSTI/ICCP/REG(2016)1/FINAL/En/pdf

Oliveira, A. S. (2019). Aspectos jurídicos da segurança cibernética no Brasil. *Revista Brasileira de Políticas Públicas*. https://www.revistapoliticaspublicas.com.br

Oliveira, S. A. (2016). La ciberseguridad en América Latina: desafíos y oportunidades. *Revista Latinoamericana de Seguridad Informática,* 8(1), 45-60. https://revistas.unal.edu.co/index.php/rlsi/article/view/56591

Santos, L. F. (2013). La ONU y la seguridad cibernética: una revisión de las iniciativas internacionales. *Revista de Estudios Internacionales, 4*(2), 75-90. http://www.revistaestudiosinternacionales.com/index.php/revista/article/view/49

Silva, L. P. (2020). A evolução dos ciberataques e suas implicações jurídicas. *Revista de Direito Internacional*. https://www.revistadireitointernacional.com.br

UN Secretary General & Group of Governmental Experts on Developments in the Field of Information and Telecommunications [GGE]. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations General Assembly. https://digitallibrary.un.org/record/799853?ln=es&v=pdf

UNIVERSIDAD
La Gran Colombia

FACULTAD DE
DERECHO
Y CIENCIAS POLITÍCAS
Y SOCIALES