Polo del Conocimiento

Pol. Con. (Edición núm. 101) Vol. 9, No 12
Diciembre 2024, pp. 2203-2212
ISSN: 2550 - 682X
DOI: 10.23857/pc.v9i12.8613

Crímenes Cibernéticos como Nuevas Formas de Delitos Internacionales: Retos para el Derecho Penal Internacional

Cybercrime as New Forms of International Crime: Challenges for International Criminal Law

Os cibercrimes como novas formas de crimes internacionais: desafios para o direito penal internacional

Jorge Guillermo Cedeño León [I]
jorge.cedenol@ug.edu.ec
https://orcid.org/0000-0002-7493-0863

Angie Gabriela Sánchez Erazo [II]
ab.angiesanchezerazo@hotmail.com
https://orcid.org/0000-0003-4050-7298

Aura Marina Lemos Espinoza [III]
abgmarinalemos@gmail.com
https://orcid.org/0000-0002-7342-4977

Christian Luvin Quito Carpio [IV]
christianquitoo@hotmail.com
https://orcid.org/0009-0009-6511-8097

Elvis Guillermo Fuentes Tenorio [V]
elvis.fuentest@ug.edu.ec
https://orcid.org/0000-0001-5445-5404

Juan Ángel Jimenez Guartán [VI]
juan.jimenezgu@ug.edu.ec
https://orcid.org/0009-0007-8214-2633

Correspondencia: jorge.cedenol@ug.edu.ec

Ciencias Sociales y Políticas
Artículo de Investigación

*** Recibido:** 26 de octubre de 2024 ***Aceptado:** 24 de noviembre de 2024 *** Publicado:** 27 de diciembre de 2024

I. Abogado, Magíster, Docente e Investigador de la Universidad de Guayaquil UG, Ecuador.
II. Abogada, Magíster, Docente e Investigador Independiente, Ecuador.
III. Abogada, Magíster, Docente e Investigador Independiente, Ecuador.
IV. Abogado, Magíster, Docente e Investigador Independiente, Ecuador.
V. Abogado, Magíster, Docente e Investigador de la Universidad de Guayaquil UG, Ecuador.
VI. Abogado, Magíster, Docente e Investigador de la Universidad de Guayaquil UG, Ecuador.

Resumen

El artículo analiza los crímenes cibernéticos como nuevas formas de delitos internacionales, destacando su impacto en la seguridad global y los desafíos que plantean para el Derecho Penal Internacional. Se examinan casos emblemáticos, normativas internacionales y avances tecnológicos, así como las lagunas jurídicas que dificultan su regulación. A través de un enfoque interdisciplinario, se proponen soluciones para fortalecer la cooperación internacional y mejorar los marcos legales existentes.

Palabras Clave: crímenes cibernéticos; delitos internacionales; Derecho Penal Internacional; seguridad global; regulación.

Abstract

The article analyses cybercrimes as new forms of international crime, highlighting their impact on global security and the challenges they pose for International Criminal Law. It examines emblematic cases, international regulations and technological developments, as well as the legal loopholes that hinder their regulation. Through an interdisciplinary approach, solutions are proposed to strengthen international cooperation and improve existing legal frameworks.

Keywords: cybercrime; international crimes; international criminal law; global security; regulation.

Resumo

O artigo analisa os cibercrimes como novas formas de crimes internacionais, destacando o seu impacto na segurança global e os desafios que representam para o Direito Penal Internacional. São examinados casos emblemáticos, regulamentos internacionais e avanços tecnológicos, bem como as lacunas legais que dificultam a sua regulamentação. Através de uma abordagem interdisciplinar, são propostas soluções para reforçar a cooperação internacional e melhorar os quadros jurídicos existentes.

Palavras-chave: crimes cibernéticos; crimes internacionais; Direito Penal Internacional; segurança global; regulamento.

Introducción

En un mundo cada vez más interconectado, los crímenes cibernéticos han emergido como una de las principales amenazas para la seguridad internacional. Desde ataques de ransomware que paralizan infraestructuras críticas hasta campañas de desinformación que socavan democracias, estos delitos han trascendido las fronteras físicas y desafiado las capacidades tradicionales del Derecho Penal Internacional.

La naturaleza transnacional de los crímenes cibernéticos complica su regulación, ya que los perpetradores suelen operar desde jurisdicciones donde las normativas son laxas o inexistentes. Según un informe de INTERPOL (2022), los ataques cibernéticos aumentaron un 70% durante la última década, afectando tanto a Estados como a empresas privadas y ciudadanos comunes (p. 15). Además, la falta de una definición universalmente aceptada de "crímenes cibernéticos" y la ausencia de un marco jurídico internacional específico han generado vacíos legales significativos. Instrumentos como la Convención de Budapest (2001) intentan abordar este problema, pero su alcance es limitado y no cuenta con la adhesión de todos los Estados clave, como Rusia o China.

El presente trabajo tiene como objetivo analizar los retos que los crímenes cibernéticos plantean para el Derecho Penal Internacional. A través de una revisión exhaustiva de normativas, doctrinas y casos concretos, se busca ofrecer un marco integral para comprender esta problemática y proponer soluciones viables.

Se abordarán temas como la necesidad de cooperación internacional, los avances en ciberseguridad y los dilemas éticos que surgen al tratar de equilibrar la seguridad global con los derechos fundamentales, como la privacidad. Finalmente, el artículo plantea la importancia de desarrollar un tratado internacional específico que armonice los esfuerzos de los Estados para combatir este fenómeno de manera efectiva.

MARCO TEÓRICO Y ESTADO DEL ARTE

1. Concepto y Características de los Crímenes Cibernéticos

Los crímenes cibernéticos, también conocidos como delitos informáticos, abarcan una amplia gama de actividades delictivas realizadas utilizando tecnologías digitales como computadoras, redes y dispositivos móviles. Estos delitos pueden clasificarse en dos categorías principales:

1. **Delitos contra sistemas informáticos:** Incluyen actividades como el hacking, ataques de denegación de servicio (DDoS), ransomware y propagación de malware, cuyo objetivo principal es comprometer la funcionalidad de infraestructuras tecnológicas.
2. **Delitos facilitados por la tecnología:** Incluyen delitos tradicionales adaptados al entorno digital, como el fraude, la explotación infantil, el robo de identidad y la difusión de información falsa (fake news).

Según Clough (2015), los crímenes cibernéticos presentan tres características esenciales:

- **Anonimato:** Los perpetradores pueden ocultar su identidad mediante herramientas como redes privadas virtuales (VPN) y el uso de la dark web, dificultando su localización (p. 38).
- **Alcance transnacional:** La naturaleza global de internet permite que los delincuentes operen desde cualquier lugar del mundo, evadiendo jurisdicciones legales específicas.
- **Rapidez de ejecución:** Los ataques pueden llevarse a cabo en cuestión de segundos, comprometiendo grandes cantidades de datos o sistemas enteros en tiempo récord.

Entre las formas más comunes de crímenes cibernéticos se encuentran:

- **Ransomware:** Programas maliciosos que cifran los datos de una víctima y exigen un rescate económico para desbloquearlos. Casos como el ataque WannaCry (2017) han afectado a miles de organizaciones, incluidas infraestructuras críticas como hospitales.
- **Phishing:** Técnicas de ingeniería social diseñadas para engañar a las personas y obtener información confidencial, como credenciales bancarias. Según un informe de INTERPOL (2022), el phishing fue el método más utilizado para el robo de datos personales durante la pandemia de COVID-19 (p. 15).
- **Ataques DDoS:** Saturación de servidores mediante múltiples solicitudes simultáneas, lo que interrumpe servicios digitales esenciales. Un ejemplo es el ataque masivo a Estonia en 2007, que paralizó instituciones gubernamentales y bancarias.

2. Principios Fundamentales del Derecho Penal Internacional Aplicados a los Crímenes Cibernéticos

El Derecho Penal Internacional proporciona un marco conceptual para abordar los crímenes cibernéticos, adaptando sus principios tradicionales a este nuevo ámbito:

1. **Responsabilidad Penal Individual:** Este principio garantiza que los individuos responsables de crímenes internacionales puedan ser procesados, incluso en el ámbito digital. Aunque los Estados pueden facilitar o

Pol. Con. (Edición núm. 101) Vol. 9, No 12, Diciembre 2024, pp. 2203-2212, ISSN: 2550 - 682X

permitir ataques cibernéticos, las personas que diseñan, ejecutan o coordinan estos delitos son responsables de sus acciones. Según Floridi (2019), este principio refuerza la idea de que el anonimato en internet no exime de la responsabilidad penal (p. 67).

2. **Universalidad:**

   Los crímenes cibernéticos que amenazan la seguridad global, como el terrorismo cibernético, pueden ser perseguidos por cualquier Estado, independientemente de dónde se cometieron. Este principio es crucial dado el carácter transnacional de estos delitos.

3. **Imprescriptibilidad:**

   Dado su impacto duradero en la seguridad internacional, los crímenes cibernéticos de gran escala, como los ataques a infraestructuras críticas, no prescriben, permitiendo su persecución en cualquier momento.

3. Normativa Internacional y Jurisprudencia

Aunque existen esfuerzos internacionales para regular los crímenes cibernéticos, el marco legal actual presenta importantes lagunas:

- **Convención de Budapest (2001):**

Es el primer tratado internacional que aborda los delitos cibernéticos, proporcionando directrices para la cooperación transfronteriza y la armonización de legislaciones nacionales. Sin embargo, su alcance es limitado, ya que no todos los países clave (como Rusia y China) son signatarios.

- **Resolución 73/27 de la ONU (2018):**

Esta resolución promueve la cooperación internacional en ciberseguridad y la creación de capacidades nacionales para prevenir crímenes cibernéticos. Sin embargo, su carácter no vinculante limita su efectividad.

- **Caso Stuxnet (2010):**

Considerado el primer ciberarma conocida, Stuxnet fue un ataque dirigido a las instalaciones nucleares de Irán. Este caso demostró la capacidad de los crímenes cibernéticos para causar daños físicos y subrayó la necesidad de un marco legal específico para regular el uso de ciberarmas (Clough, 2015, p. 48).

4. Experiencias Internacionales

1. **Estonia (2007):**

Este ataque cibernético masivo, atribuido a actores estatales, paralizó infraestructuras críticas y demostró la vulnerabilidad de los Estados frente a las ciberamenazas. Estonia respondió

desarrollando capacidades avanzadas de ciberseguridad y promoviendo la cooperación internacional, convirtiéndose en líder en el ámbito de la defensa cibernética.

2. **Corea del Norte y WannaCry (2017):**

El ataque de ransomware WannaCry, atribuido al grupo Lazarus patrocinado por Corea del Norte, afectó a más de 150 países y destacó el uso de crímenes cibernéticos como herramienta de presión internacional.

3. **SolarWinds (2020):**

Este ataque dirigido a empresas y agencias gubernamentales de Estados Unidos subrayó la sofisticación de los ciberataques patrocinados por Estados y la necesidad de fortalecer la cooperación internacional en ciberseguridad.

5. Desafíos y Críticas

1. **Vacíos Legales:**

La falta de definiciones uniformes y tratados vinculantes dificulta la persecución efectiva de crímenes cibernéticos. Por ejemplo, mientras algunos países consideran los ataques cibernéticos como actos de guerra, otros los clasifican como delitos comunes.

2. **Falta de Cooperación Internacional:**

La falta de consenso entre Estados clave sobre cómo regular los crímenes cibernéticos ha obstaculizado la creación de un marco normativo global.

3. **Impacto Ético:**

El uso de herramientas de vigilancia masiva para prevenir delitos cibernéticos plantea dilemas éticos significativos. Según Floridi (2019), es fundamental garantizar que estas herramientas respeten los derechos fundamentales, como la privacidad y la libertad de expresión (p. 74).

4. **Evolución Tecnológica:**

El desarrollo constante de nuevas tecnologías, como la inteligencia artificial y la computación cuántica, plantea retos adicionales para el Derecho Penal Internacional, que debe adaptarse rápidamente a estos cambios.

METODOLOGÍA

1. **Método Descriptivo:**

Este método permite identificar las características principales de los crímenes cibernéticos y su evolución dentro del marco del Derecho Penal Internacional. A través de este enfoque, se analiza

el impacto de estos delitos en diferentes contextos sociales, económicos y políticos, detallando los principales desafíos legales y las estrategias de mitigación implementadas por los Estados.

2. **Método Bibliográfico:**

Se lleva a cabo una revisión exhaustiva de tratados internacionales como la Convención de Budapest (2001), literatura académica especializada, y casos judiciales emblemáticos como Stuxnet y WannaCry. Este método proporciona una base teórica sólida para sustentar las propuestas y conclusiones del estudio, vinculando las normativas existentes con los desafíos actuales de los crímenes cibernéticos.

3. **Método Fenomenológico Jurídico:**

El análisis de casos concretos como el ataque a Estonia en 2007 y SolarWinds en 2020 permite evaluar la implementación práctica de normativas internacionales y el impacto de estas en la prevención y sanción de delitos cibernéticos. Este enfoque también explora las experiencias vividas por Estados y organizaciones afectadas, destacando fortalezas y áreas de mejora en la respuesta a estas amenazas.

RESULTADOS Y DISCUSIÓN

1. Definición y Ejemplos de Implementación

Tabla 1: Casos emblemáticos y su impacto jurídico

Caso	Impacto Jurídico	Contribución
Estonia (2007)	Evidenció la vulnerabilidad de infraestructuras	Impulso a la creación de políticas de ciberseguridad avanzada.
WannaCry (2017)	Uso del ransomware como herramienta estatal.	Aceleró el debate global sobre ciberdefensa y cooperación.
SolarWinds (2020)	Infiltración masiva en sistemas corporativos.	Subrayó la necesidad de cooperación internacional efectiva.

Los casos mencionados destacan la creciente sofisticación de los crímenes cibernéticos y su capacidad de impactar tanto a Estados como a corporaciones globales. Por ejemplo, el ataque a Estonia llevó a la creación del Centro de Excelencia en Defensa Cibernética de la OTAN, mientras que WannaCry generó un aumento en la inversión en ciberseguridad a nivel mundial.

2. Cuestiones Éticas

El combate a los crímenes cibernéticos plantea dilemas éticos significativos, particularmente en relación con la vigilancia masiva y la privacidad. Según Floridi (2019), el equilibrio entre seguridad y derechos fundamentales debe ser central en cualquier estrategia de prevención. La recopilación de datos a gran escala para identificar posibles amenazas puede derivar en abusos, como la discriminación algorítmica o la violación de la privacidad de los ciudadanos (p. 65).

Además, el uso de inteligencia artificial para identificar patrones de conducta delictiva en internet plantea interrogantes sobre la transparencia y la rendición de cuentas de los sistemas automatizados, así como sobre la posible marginación de comunidades vulnerables.

3. Regulación y Normativas Necesarias

A pesar de la existencia de la Convención de Budapest, el marco normativo global sigue siendo insuficiente para abordar la complejidad de los crímenes cibernéticos. Los vacíos legales incluyen:

- Falta de definiciones uniformes para delitos específicos como el terrorismo cibernético.
- Ausencia de mecanismos vinculantes que obliguen a los Estados a cooperar en la investigación y persecución de delitos transnacionales.

La creación de un tratado internacional vinculante, basado en principios como la universalidad y la responsabilidad compartida, podría fortalecer la capacidad de los Estados para combatir estas amenazas.

4. Estudios de Caso y Experiencias Internacionales

Estonia (2007): Este ataque masivo evidenció la vulnerabilidad de las infraestructuras digitales estatales y marcó un punto de inflexión en la percepción de las ciberamenazas. Estonia respondió con la creación de una estrategia nacional de ciberseguridad, convirtiéndose en líder en este ámbito a nivel global.

WannaCry (2017): Este ataque ransomware, atribuido a actores estatales, demostró la capacidad de los crímenes cibernéticos para causar daños a gran escala. Afectó a hospitales, bancos y empresas en más de 150 países, acelerando los esfuerzos para desarrollar marcos legales y operativos de ciberdefensa.

SolarWinds (2020): Este caso resaltó las debilidades en las cadenas de suministro de software, subrayando la necesidad de una cooperación más estrecha entre el sector público y privado para prevenir infiltraciones en infraestructuras críticas.

Pol. Con. (Edición núm. 101) Vol. 9, No 12, Diciembre 2024, pp. 2203-2212, ISSN: 2550 - 682X

CONCLUSIONES

1. Los crímenes cibernéticos representan un desafío significativo para el Derecho Penal Internacional debido a su naturaleza transnacional y rápida evolución.
2. A pesar de los avances logrados, como la Convención de Budapest, es evidente la necesidad de un marco normativo global más integral y vinculante.
3. La cooperación internacional es esencial para enfrentar estas amenazas, especialmente en el intercambio de información y recursos para la prevención y persecución de delitos cibernéticos.
4. Los Estados deben equilibrar las estrategias de ciberseguridad con la protección de los derechos fundamentales, evitando abusos que puedan comprometer la confianza pública.
5. Las experiencias de casos emblemáticos demuestran que la preparación y la respuesta proactiva son claves para mitigar el impacto de los crímenes cibernéticos.

RECOMENDACIONES

1. Promover un Tratado Internacional Vinculante: Diseñar un marco legal que defina de manera uniforme los crímenes cibernéticos y establezca obligaciones claras para los Estados.
2. Fortalecer las Capacidades de Ciberseguridad: Invertir en tecnologías avanzadas y formación especializada para prevenir y responder a amenazas cibernéticas.
3. Fomentar la Cooperación Público-Privada: Impulsar alianzas entre gobiernos y empresas tecnológicas para desarrollar soluciones innovadoras y resilientes.
4. Asegurar el Respeto a los Derechos Fundamentales: Establecer salvaguardas éticas y legales para garantizar que las estrategias de prevención no vulneren derechos como la privacidad y la libertad de expresión.

Impulsar la Concienciación Ciudadana: Implementar campañas de educación sobre ciberseguridad para empoderar a los usuarios en la protección de sus datos y sistemas.

Referencias

- Caso SolarWinds (2020). Análisis del ataque a sistemas corporativos y gubernamentales.
- Caso Estonia (2007). Impacto del ciberataque en políticas estatales de ciberseguridad.
- Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.
- Convención de Budapest. (2001). Tratado sobre Ciberdelincuencia. Consejo de Europa.
- European Union Agency for Cybersecurity (ENISA). (2021). Threat Landscape Report.
- Floridi, L. (2019). Ethics in the Age of Information. Oxford University Press.
- Guitton, C. (2013). The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. Routledge.
- INTERPOL. (2022). Global Crime Trends: Cybercrime Report.
- ONU. (2018). Resolución 73/27 sobre Cooperación Internacional en Ciberseguridad.
- ONU. (2019). The Age of Digital Interdependence. High-Level Panel on Digital Cooperation.
- Smith, A. G. (2020). International Cybersecurity Law: Legal, Political and Technological Dimensions. Palgrave Macmillan.
- WannaCry (2017). Ataque Ransomware. Estudio sobre los efectos globales y atribuciones al grupo Lazarus..