ISSN 3008-9484 | DOI 10.5281/zenodo.17967380 **Diálogos y Voces Judiciales |** Vol. 2, Núm. 3 (diciembre de 2025): 72-92

CIBERSEGURIDAD Y GOBERNANZA GLOBAL: ENTRE BUDAPEST Y LA PROPUESTA DE NACIONES UNIDAS

Cybersecurity and Global Governance: Between Budapest and the United Nations Proposal

Rosa Merlín Rodríguez[*]

Universidad Nacional Autónoma de México

rmerlin@politicas.unam.mx

https://orcid.org/0009-0001-0191-4060

RECIBIDO 14/11/2025 - ACEPTADO 17/11/2025

Resumen

El artículo compara el Convenio de Ciberdelincuencia del Consejo de Europa con la propuesta de Convención de la ONU. El Convenio ofrece procedimientos penales armonizados y cooperación ágil, pero su alcance regional y enfoque tecnocrático limitan su legitimidad y amplían tendencias punitivas. La Convención de la ONU aspira a legitimidad universal y mayor centralidad de los derechos humanos, aunque enfrenta obstáculos políticos y operativos. El trabajo propone un modelo de gobernanza híbrida que combine interoperabilidad técnica, sólidas salvaguardas de derechos y mecanismos multilaterales inclusivos para reducir desigualdades y fortalecer la ciberseguridad como herramienta de cooperación y justicia.

Palabras clave:

ciberespacio, ciberseguridad, convenciones, gobernanza, ciberdelincuencia.

Abstract

The article compares the Council of Europe's Cybercrime Convention with the United Nations' proposal. The Convention offers harmonized criminal procedures and swift operational cooperation, but its regional scope and technocratic orientation limit its legitimacy and reinforce punitive approaches. The UN proposal seeks universal legitimacy and a stronger human rights focus, yet faces significant political and operational challenges. The article advocates for a hybrid governance model that combines technical interoperability, robust human rights safe-guards, and inclusive multilevel mechanisms to reduce inequalities and strengthen cybersecurity as a tool for cooperation and justice.

Keywords:

cyberspace, cybersecurity, conventions, governance, cybercrime.

1. Introducción

La seguridad hemisférica contemporánea se ha configurado bajo una lógica marcadamente multidimensional. Fenómenos como la transnacionalidad del crimen organizado, el terrorismo, el desarrollo acelerado de las tecnologías digitales y la expansión de internet no solo han redefinido la agenda internacional, sino que han colocado a la ciberseguridad como uno de los componentes estructurales del orden global. Esta transformación vuelve indis-

[*] Lic. en Derecho (Universidad Nacional Autónoma de México), Doctora en Derecho y Gobernanza Global (Universidad de Salamanca). Académica de la Facultad de Ciencias Políticas y Sociales de la UNAM.

pensable su estudio desde las Relaciones Internacionales, disciplina para la cual el ciberespacio constituye hoy un ámbito crítico de disputa de poder, regulación y legitimidad.

En América Latina, la construcción del sistema interamericano durante la Guerra Fría, articulada en torno al Tratado Interamericano de Asistencia Recíproca (TIAR) y la Organización de los Estados Americanos (OEA en adelante) y el liderazgo hegemónico de Estados Unidos configuró una noción de seguridad centrada inicialmente en amenazas estatales convencionales. No obstante, desde la fundación de la Junta Interamericana de Defensa (JID de ahora en adelante) en 1942 hasta la Declaración de Bridgetown de 2002, dicha noción ha evolucionado de forma sustancial. El punto de inflexión se produjo durante la Conferencia Especial de Seguridad celebrada en México en 2003, donde los Estados miembros de la OEA ampliaron el concepto de seguridad hacia un enfoque multidimensional, incorporando amenazas no tradicionales como: el terrorismo, la delincuencia transnacional y, de manera creciente, los ataques a la seguridad cibernética.

En este marco, la OEA a través del Comité Interamericano contra el Terrorismo (CICTE de ahora en adelante) ha incentivado la cooperación entre gobiernos, sector privado y sociedad civil para identificar vulnerabilidades y diseñar políticas nacionales en materia de ciberseguridad (Ibarra y Nieves, 2016). Estas acciones responden a una realidad contundente: las amenazas que emergen en el ciberespacio han reconfigurado drásticamente los paradigmas clásicos de seguridad internacional. A diferencia de los conflictos armados localizables territorialmente, las ciberamenazas se caracterizan por su deslocalización, su naturaleza multifacética y su rápida mutación.

Esta complejidad erosiona categorías jurídicas tradicionales como agresión, soberanía y responsabilidad internacional, que se ven tensionadas por la dificultad para atribuir ataques y por la presencia simultánea de actores estatales y no estatales operando desde múltiples jurisdicciones (Robles, 2016). El espectro de amenazas incluye desde delitos informáticos comunes como el fraude, robo de datos, explotación sexual infantil en línea hasta actividades más sofisticadas como el ciberespionaje estatal, el sabotaje digital y las acciones contra infraestructuras críticas. La distinción clásica entre cibercrimen, ciberterrorismo y ciberguerra se vuelve así insuficiente para dar cuenta de fenómenos que pueden superponer tácticas, actores y motivaciones en un mismo evento.

Los reportes recientes confirman esta tendencia. El "Global Threat Report 2024" de CrowdStrike registra un incremento del 60% en intrusiones interactivas durante 2023 y un aumento del 73 % en el segundo semestre, con el sector tecnológico como principal objetivo. Este patrón se intensificó durante la pandemia, cuando la digitalización masiva aumentó la superficie de ataque global. De manera paralela, el Fondo Monetario Internacional (2024) alerta sobre el riesgo de que los ciberataques funcionen como detonadores de crisis macrofinancieras, especialmente en sectores altamente digitalizados como el financiero.

Sin embargo, la problemática no es nueva. Desde el uso fraudulento del telégrafo en el siglo XIX hasta los *phreakers* de la década de 1970 que manipulaban sistemas telefónicos mediante *blue boxes*, la historia revela que la innovación tecnológica ha sido sistemáticamente acompañada de nuevas formas de criminalidad (Sain, 2018). La "Operación Diablo del Sol" de 1990, aunque con limitados efectos legales, constituye uno de los primeros precedentes de cooperación internacional contra la delincuencia informática (OGDI,

2016). La liberalización del comercio global en los años noventa propició aún más la expansión del cibercrimen transfronterizo, particularmente en el ámbito financiero (Sain, 2015).

Las Tecnologías de la Información y la Comunicación (TIC en adelante) han transformado la naturaleza de los delitos al ofrecer anonimato, bajo costo, alcance global y facilidad técnica. Esta evolución, señala Bartolomé (2020), reduce la barrera de entrada para los atacantes, diluye las fronteras jurídicas, dificulta la detección de incidentes y vuelve ineficaces los modelos clásicos de análisis del crimen. Zunzunegui agrega que la deslocalización y la existencia de jurisdicciones permisivas configuran "paraísos cibernéticos", donde la persecución penal resulta prácticamente inviable (2008, p. 171).

Este panorama evidencia la necesidad urgente de contar con marcos normativos de alcance global que sean capaces de responder a la escala, la velocidad y la sofisticación de las amenazas contemporáneas en el ciberespacio. En este contexto, resulta particularmente relevante la comparación entre dos modelos internacionales de respuesta: el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest de ahora en adelante), y la Convención de las Naciones Unidas contra la Ciberdelincuencia. Ambos instrumentos encarnan concepciones divergentes de gobernanza digital y revelan tensiones geopolíticas, conceptuales y de derechos humanos que atraviesan el debate actual sobre la regulación del entorno digital.

El Convenio de Budapest, vigente desde 2004, constituye el marco jurídico internacional más consolidado en la materia. Su aportación principal radica en la armonización de tipos penales, el establecimiento de procedimientos claros para la preservación y obtención de datos, la creación de mecanismos ágiles de cooperación operativa y el desarrollo de herramientas técnicas con más de dos décadas de aplicación acumulada. Estas características le otorgan estabilidad jurídica y una valiosa experiencia institucional. Sin embargo, su naturaleza regional y su fuerte orientación tecnocrática, así como su origen asociado a estándares impulsados predominantemente por Estados occidentales, han suscitado recelo entre diversos países del Sur Global. Para muchos de ellos, el Convenio continúa siendo insuficientemente universal y excesivamente inclinado hacia paradigmas punitivos y de vigilancia, lo que ha limitado su aceptación y ha reforzado críticas sobre su sesgo geopolítico.

En contraste, la propuesta de Convención de la Organización de las Naciones Unidas (ONU en adelante) se presenta como un esfuerzo por construir un marco verdaderamente universal, sustentado en un enfoque más amplio que incorpora la protección robusta de derechos humanos, principios de gobernanza inclusiva, el reconocimiento expreso de la soberanía digital y la articulación de mecanismos de cooperación multinivel. Aun así, este proyecto enfrenta desafíos significativos. Entre los más relevantes se encuentran las profundas divergencias políticas entre los distintos bloques de Estados, el riesgo de generar instrumentos sobrerregulatorios o susceptibles de politización, las dificultades técnicas inherentes a la armonización de estándares globales y la preocupación de que algunos gobiernos utilicen la ampliación de tipos penales como herramienta para restringir derechos fundamentales, reprimir la disidencia o limitar libertades en el espacio digital.

2. Formas de amenazas en el ciberespacio

La consolidación del ciberespacio como un dominio autónomo de interacción social, económica y política ha catalizado el surgimiento de nuevas formas de conflictividad que transgreden las categorías tradicionales del Derecho Internacional y desbordan los marcos normativos diseñados para regir escenarios físicos. En este sentido, la Estrategia Nacional de Ciberseguridad de España (2019) identifica tres manifestaciones paradigmáticas que configuran los principales focos de riesgo estructural en el entorno digital contemporáneo: el cibercrimen, el ciberterrorismo y la ciberguerra (Gutiérrez, 2020, p. 17). Estos fenómenos no sólo constituyen desafíos a la soberanía y la seguridad estatal, sino que también exigen un replanteamiento profundo de las herramientas jurídicas, institucionales y doctrinales aplicables a los conflictos digitales.

El cibercrimen, en su expresión más extendida, se refiere a conductas delictivas que se cometen mediante el uso de sistemas informáticos o contra estos, con una finalidad predominantemente lucrativa. Entre sus múltiples formas destacan las extorsiones realizadas a través de *ransomware*, el acceso no autorizado a bases de datos, la suplantación de identidad con fines de fraude (*phishing*), la distribución de malware para el robo o la manipulación de información, así como los ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), que comprometen la operatividad de infraestructuras esenciales. Si bien la lógica económica es dominante, el cibercrimen no excluye móviles ideológicos o geoestratégicos, lo que evidencia una difuminación creciente de sus límites con otras expresiones de amenaza digital.

Por su parte, el ciberterrorismo representa una forma de violencia cuyo objetivo no es el beneficio material, sino la producción de efectos simbólicos o políticos, mediante el uso sistemático de las tecnologías digitales para generar miedo, subvertir el orden público o desestabilizar estructuras institucionales. En esta categoría se incluyen tanto el sabotaje informático contra servicios esenciales como redes eléctricas, sistemas de salud o transporte, como la propagación de contenidos extremistas, el reclutamiento virtual de simpatizantes o la planificación de actos de violencia mediante plataformas cifradas. Su carácter disruptivo no reside sólo en el daño técnico causado, sino en su capacidad para erosionar la confianza social y debilitar los pilares normativos del Estado constitucional.

La ciberguerra, finalmente, constituye la manifestación más sofisticada y potencialmente destructiva de la conflictividad interestatal en el ciberespacio. A diferencia del ciberterrorismo o el crimen digital, aquí predomina la racionalidad estratégica de los Estados, que emplean capacidades ofensivas y defensivas cibernéticas como herramientas de proyección de poder, interferencia política o coerción indirecta. Estas operaciones –que pueden desplegarse de manera encubierta o abierta, autónoma o combinada con medios cinéticos– buscan alterar el equilibrio de poder internacional mediante la neutralización de infraestructuras críticas, la manipulación de procesos electorales o la interrupción de servicios soberanos. Conforme al Manual de Tallin sobre el Derecho Internacional aplicable a la Ciberguerra, este tipo de agresiones puede alcanzar la categoría de "uso de la fuerza" o "ataque armado" si sus efectos materiales son equiparables a los previstos en el artículo 51 de la Carta de las Naciones Unidas.

Estas tres formas no deben entenderse como compartimentos estancos, sino como tipos analíticos que comparten tecnologías, actores, plataformas y tácticas. La intersección de motivaciones políticas, económicas y militares da lugar a escenarios híbridos que desafían la capacidad del Derecho Internacional para clasificar, atribuir y sancionar adecuadamente estas conductas. En este contexto, la elaboración de una arquitectura jurídica coherente y eficaz exige superar las lógicas binarias propias del derecho penal clásico o del *ius ad bellum*, adoptando enfoques multidimensionales que integren elementos del Derecho Internacional humanitario, del Derecho Penal Internacional, de la protección de los derechos humanos y del régimen de cooperación interestatal.

El debate doctrinal ha intentado dar respuesta a este desafío mediante la proliferación de términos como ciberdelito, criminalidad informática o delincuencia digital, sin que hasta el momento se haya alcanzado una definición jurídica consolidada a nivel global. Esta dispersión terminológica no es meramente semántica: refleja la ausencia de consensos sobre los elementos normativos, sustantivos y procesales que deben estructurar el régimen internacional de combate a las amenazas digitales. Esta ambigüedad conceptual obstaculiza la armonización de legislaciones nacionales, debilita los marcos de cooperación judicial transfronteriza y favorece la impunidad, especialmente en contextos donde los Estados se muestran renuentes a tipificar estos actos o carecen de voluntad política para sancionarlos eficazmente.

En consecuencia, resulta indispensable avanzar hacia una sistematización jurídica del ciberconflicto, que articule marcos normativos robustos con mecanismos institucionales de coordinación y rendición de cuentas. Frente a una conflictividad que evoluciona con velocidad tecnológica y que erosiona silenciosamente la estabilidad del orden jurídico internacional, el Derecho está llamado no solo a reaccionar, sino a anticipar y regular con visión transformadora, en defensa de la paz, la legalidad y los derechos fundamentales en el entorno digital global.

Hasta ahora, la mayor parte de la legislación internacional sobre ciberdelitos ha priorizado la criminalización como principal respuesta: tipificar nuevas conductas delictivas o adaptar las ya existentes para enfrentar los retos del ciberespacio. Sin embargo, este enfoque resulta limitado. El Convenio de Budapest (2001) fue pionero al intentar ofrecer un marco más integral, que no solo incluyera delitos sustantivos, sino también normas procesales y mecanismos de cooperación internacional. Sus categorías abarcan ataques contra la confidencialidad, integridad y disponibilidad de datos, fraudes informáticos, delitos de contenido (como la pornografía infantil) e infracciones a derechos de autor.

A pesar de su resiliencia capaz de adaptarse a nuevas modalidades delictivas como las *botnets*, el instrumento deja vacíos importantes: el robo de identidad, el *grooming* a menores, el *spam* y el ciberterrorismo no fueron contemplados. Estas omisiones responden tanto a dificultades técnicas como a divergencias socioculturales. Por ejemplo, mientras que algunos países en desarrollo buscan penalizar el spam, las economías avanzadas lo tratan como un problema civil o administrativo. De este modo, el Convenio refleja un consenso mínimo más que un marco global comprehensivo. Además, su origen europeo y la falta de adhesión de potencias clave han limitado su legitimidad y alcance universal.

3. Perspectivas conceptuales de la ciberseguridad

El concepto de ciberseguridad, aunque relativamente reciente, abarca prácticas de seguridad informática que han evolucionado con el tiempo. Sin embargo, su definición es aún motivo de debate entre los Estados. Lo que antes se consideraba un asunto técnico limitado a la gestión de riesgos en infraestructuras críticas, hoy se ha convertido en una prioridad estratégica para la seguridad nacional. A medida que la digitalización avanza y transforma la economía, la sociedad y la política, las preocupaciones en torno a la ciberseguridad continúan creciendo, consolidando su papel central en la gobernanza global del ciberespacio.

Esta se ha consolidado como un eje central en la agenda política global, trascendiendo su impacto inicial en el ámbito estatal y empresarial para convertirse en un elemento clave de la geopolítica contemporánea. Como señalan Dunn Cavelty y Wenger (2019), su alcance se ha expandido hacia una multiplicidad de esferas políticas, reflejando su creciente complejidad y la interconexión con cuestiones estratégicas más amplias. Este fenómeno evidencia que la ciberseguridad ya no puede abordarse únicamente desde una perspectiva técnica, sino que requiere un enfoque integral que considere sus implicaciones en la seguridad nacional, la economía digital y la gobernanza global del ciberespacio.

Según Josep Ibañez (2011), surge como una respuesta indispensable para contrarrestar las amenazas originadas en el ciberespacio, un ámbito donde interactúan actores diversos en un entramado complejo. Esta dinámica demanda un enfoque de gobernanza que logre equilibrar los distintos intereses involucrados, tales como la protección de datos, la seguridad nacional y las libertades individuales.

En este contexto, la seguridad cibernética se convierte en un campo de disputa y cooperación entre diferentes actores, reflejando las dinámicas de poder y las asimetrías globales. Maximiliano Vila y Marcelo Saguier (2019) destacan que la digitalización reconfigura las relaciones de poder, dando paso a nuevas formas de hegemonía digital, donde los actores dominantes se benefician de un control creciente sobre el ciberespacio.

Ésta es entendida como el esfuerzo por salvaguardar la integridad de los sistemas digitales, la confidencialidad de la información y la disponibilidad de infraestructuras. La ciberseguridad se ha consolidado como una cuestión crítica tanto en el ámbito privado como público, tal como proponen Singer y Friedman (2014). En el sector empresarial, resulta esencial para mantener la eficiencia y rentabilidad sin comprometer la seguridad de empleados y clientes. A nivel estatal, sin embargo, ha adquirido un carácter prioritario, convirtiéndose en una cuestión de seguridad nacional.

Vargas y Recalde (2017) subrayan que la creciente sofisticación de los ciberataques ha obligado a los gobiernos a invertir en capacidades de ciberdefensa y a formular políticas para disuadir o responder ante estas amenazas. Este fenómeno refleja un cambio significativo hacia la ciberseguridad como una estrategia clave del Estado. En muchos casos, este enfoque se ve reforzado por una perspectiva securitizadora, donde se aborda desde una óptica militar y de defensa. Vila y Saguier (2019) critican esta hegemonía de la perspectiva estratégica, señalando cómo ha desplazado la visión libertaria original de los pioneros de internet.

El proceso de securitización de la ciberseguridad, sin embargo, no está exento de controversias. Según Vila y Saguier (2019), las nuevas formas de poder y las asimetrías generadas

en el ámbito digital revelan un orden hegemónico configurado por actores predominantes, ya sean Estados o corporaciones tecnológicas. Estos actores, al ocupar una posición central en la gobernanza digital, ejercen una influencia significativa sobre las normas y políticas que rigen el ciberespacio. No obstante, los autores también señalan que los países de América Latina, y en general aquellos que experimentan nuevas formas de dependencia tecnológica, enfrentan grandes dificultades para participar activamente en la configuración de este orden mundial digital, lo que evidencia una brecha en la gobernanza global que debe ser abordada.

Los enfoques de Ibáñez (2011), Singer y Friedman (2014), Vargas y Recalde (2017), y Vila y Saguier (2019) nos presentan un escenario complejo en el que las dinámicas de poder, las vulnerabilidades cibernéticas y las estrategias de seguridad nacional convergen. Este entorno globalizado e interdependiente evidencia las crecientes tensiones entre la protección de la privacidad, la soberanía digital y la seguridad colectiva. Las políticas y estrategias de ciberseguridad deben reconocer estas asimetrías y tensiones, adoptando un enfoque inclusivo que contemple no solo los intereses de los actores más poderosos, sino también los de aquellos que se ven más afectados por las dinámicas de la digitalización y la ciberseguridad global.

En la literatura de la política internacional, la ciberseguridad se presenta como un campo de creciente tensión geopolítica, donde potencias como China, Estados Unidos y Rusia desempeñan papeles clave en la formulación de sus estrategias de seguridad cibernética. Chang (2014) señala que la ciberseguridad ha dado lugar a comunidades especializadas en el pensamiento estratégico, donde China y Estados Unidos adoptan enfoques diferenciados. A medida que el ciberespacio se convierte en un nuevo terreno de disputa global, las relaciones de poder, hegemonía y soberanía digital se hacen cada vez más evidentes.

En el caso de China, la narrativa de la ciberseguridad se caracteriza por la ambición de convertirse en una potencia cibernética global, como afirma Shen (2016). Bajo el liderazgo de Xi Jinping, la ciberseguridad ha sido posicionada como un objetivo estratégico prioritario, con el propósito no solo de proteger su infraestructura, sino también de dominar el ciberespacio. Esta postura contrasta con la de Estados Unidos, que, según Ülgen (2016), enfrenta constantes ciberataques debido a su posición como superpotencia. En este contexto, Estados Unidos se ha visto obligado a desarrollar una estrategia nacional de protección de infraestructura cibernética, consolidando un enfoque de "resolución de problemas" que busca mantener el orden hegemónico neoliberal. Este modelo se refleja también en las políticas de gobernanza de internet, donde Estados Unidos promueve un modelo de múltiples partes interesadas, que busca equilibrar el poder entre actores estatales y no estatales, pero que también refleja su dominio sobre las normas internacionales.

Rosa Piñón (2018) critica que, en términos de ciberseguridad, la gobernanza global sigue siendo una tarea pendiente debido a la falta de consenso y las divergencias entre actores internacionales. La pluralidad de estrategias, junto con una regulación jurídica obsoleta, complica la creación de un marco de cooperación que permita una gobernanza efectiva en el ciberespacio. Según Piñon, la ciberseguridad no puede entenderse solo como una respuesta a las amenazas, sino como un campo donde tanto Estados como actores no estatales utilizan el ciberpoder para posicionarse y proteger sus intereses, lo que genera tensiones sobre las normas de gobernanza global.

El análisis de Ülgen (2016) también subraya la complejidad de la ciberseguridad como un ámbito de acción estatal y defensa, donde Rusia, con su legado soviético, se ha convertido en un actor clave en la ejecución de ciberataques, reflejando la rivalidad tecnológica entre las grandes potencias. En este contexto, el poder cibernético no solo está relacionado con la protección de sistemas, sino también con la afirmación de poder y soberanía en un mundo digital cada vez más interconectado.

Las perspectivas conceptuales de la ciberseguridad, como lo subrayan los distintos autores, indican que este tema no es solo una cuestión técnica, sino también una arena de conflicto geopolítico, donde las potencias emplean el ciberpoder como una extensión de su influencia y control sobre el orden mundial. Por lo que la gobernanza de la ciberseguridad debe analizarse no solo en términos de amenazas y soluciones, sino también en relación con las dinámicas de poder que subyacen a la construcción de las normas y estrategias de seguridad global.

La ciberseguridad es un campo en constante evolución que trasciende los enfoques tradicionales de análisis y demanda una perspectiva interdisciplinaria. Su impacto en la sociedad se intensificará a medida que las nuevas tecnologías digitales amplíen los límites del ciberespacio y den lugar a problemáticas aún más complejas. La interacción entre la ciberseguridad, los cambios socioeconómicos y el desarrollo del Estado plantea un desafío crucial: garantizar que las soluciones tecnológicas no solo respondan a amenazas emergentes, sino que también contribuyan a una gobernanza digital equilibrada y sostenible (Dunn Cavelty y Wenger, 2019).

El estudio de la ciberseguridad exige una perspectiva profundamente interdisciplinaria, capaz de responder a la velocidad de los cambios tecnológicos y a las transformaciones del entorno político global. Desde el ámbito jurídico, resulta indispensable comprender la ciberseguridad como un asunto de interés para el derecho y la justicia, debido a su impacto directo en la prevención de delitos y en la mitigación de afectaciones que trascienden la infraestructura crítica del Estado. Estas problemáticas incluyen la protección de datos personales, el robo de identidad, el fraude digital y otras conductas que pueden vulnerar derechos humanos fundamentales.

En este contexto, se vuelve necesario adoptar un enfoque que combine la cooperación internacional con formas de colaboración amplia entre los distintos actores que participan, inciden o resultan afectados en este ecosistema. Solo a través de esta articulación será posible construir respuestas más integrales y efectivas frente a las amenazas del ciberespacio.

4. El Convenio sobre la Ciberdelincuencia en el marco del Consejo de Europa

El Convenio sobre Ciberdelincuencia, también conocido como "Convenio de Budapest", es un tratado promovido por el Consejo de Europa en 2001 para mejorar la cooperación entre países y crear marcos legales coherentes contra la ciberdelincuencia y la actividad delictiva en internet.

En cuanto a su estructura, éste consta de 48 artículos y un preámbulo. En concreto encontramos cuatro capítulos, divididos en secciones y títulos. El primer capítulo tan sólo comprende un precepto, referido a la terminología usada en el texto. El capítulo segundo,

"Medidas que deberán adoptarse a nivel nacional", incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad, etc.) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción, etc.). En cuanto al tercero, se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

Ha sido ratificado por 31 Estados de Europa y los Estados Unidos de América con el propósito de combatir la cibercriminalidad y promover la cooperación transnacional en este ámbito. Argentina, Chile, Costa Rica, Colombia, Panamá, Paraguay, Perú y República Dominicana son los países latinoamericanos que han suscrito el Convenio, mientras que Brasil, Ecuador, Guatemala, México son observadores.

El Convenio de Budapest es ampliamente reconocido como un punto de referencia en los esfuerzos globales para fortalecer el Estado de Derecho en el ciberespacio. No solo fue el primer tratado internacional en este campo, sino que también sigue siendo uno de los instrumentos jurídicos más importantes como un modelo para naciones interesadas en elaborar leyes integrales contra los delitos cibernéticos y como un marco para la colaboración internacional entre los países que son parte de este tratado.

Entre sus aspectos clave se encuentran la tipificación como delito de acciones como el acceso no autorizado, los ataques a la integridad de sistemas y datos, el fraude informático y los delitos vinculados a la pornografía infantil. Además, ofrece herramientas legales que mejoran la efectividad de las investigaciones sobre ciberdelitos y la obtención de pruebas electrónicas, al tiempo que fomenta una cooperación internacional rápida y eficiente en este ámbito.

Sin embargo, no define específicamente el término ciberdelito o cibercrimen, sino que se centra en las conductas criminales relacionadas con la informática que los Estados parte deben incluir en sus leyes internas. En el Artículo 1 establece una serie de definiciones tales como sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico.

Los Títulos 1, 2, 3, 4 de dicho convenio establece una serie de delitos a saber:

Cuadro 1

Delitos contenidos en el Convenio sobre la Ciberdelincuencia

Clasificación	Tipo de delitos
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	Acceso ilícito Interceptación ilícita Ataques a la integridad de datos Ataques a la integridad del sistema
Delitos informáticos	Falsificación informática Fraude informático

Delitos relacionados con el contenido	Delitos relacionados con la pornografía infantil Abusos a los dispositivos
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Fuente: Elaboración propia a partir del Convenio sobre la Ciberdelincuencia. Apoyo con ChatGPT.

Como se puede observar en el Cuadro 1, estas conductas se dividen en delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos; delitos informáticos como falsificación y fraude; delitos relacionados con contenido como pornografía infantil; y delitos de propiedad intelectual y derechos afines. Además de las disposiciones penales, el convenio también abarca aspectos procesales, jurisdiccionales y un sistema detallado de cooperación internacional para combatir este tipo de crimen.

Respecto a las medidas que han de adoptarse a nivel nacional, el Convenio establece que cada país firmante debe implementar medidas legislativas y otras acciones necesarias para tipificar como delitos, en su jurisdicción nacional, los siguientes actos (Consejo de Europa, 2001):

1) Acceso deliberado e ilegítimo a todo o parte de un sistema informático (Art. 2).
2) Interpretación deliberada o legítima por medios técnicos, de datos informáticos transmitidos en comunicaciones no públicas en un sistema informático (Art. 3).
3) Ataques a la integridad de datos como todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos (Art. 4).
4) Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático (Art. 5).
5) Comisión deliberada e ilegítima de la producción, venta, obtención para uso, importación, difusión u otra forma de disponibilidad de dispositivos en programas informáticos y contraseñas, con el propósito de cometer los delitos mencionados anteriormente (Art. 6).
6) Falsificación informática, fraude informático, pornografía infantil, delitos relacionados con infracciones a la propiedad intelectual y derechos similares (Arts. 7, 8, 9 y 10).

El Convenio de Budapest también establece la penalización de delitos como la tentativa y la complicidad, así como la responsabilidad legal de las entidades jurídicas. Además, indica que las sanciones deben ser efectivas, proporcionadas y disuasorias, incluyendo penas privativas de libertad. Cada Parte del Convenio conserva la jurisdicción para juzgar delitos cometidos en su territorio, en buques o aeronaves bajo su bandera, por sus nacionales en ciertas circunstancias, o cuando ningún Estado tiene competencia territorial.

En este sentido establece un marco legal para la cooperación internacional en delitos que implican pruebas electrónicas. Va más allá de la ciberdelincuencia. Facilita la firma del Segundo Protocolo Adicional al Convenio de Budapest, mejorando la cooperación y la divulgación de pruebas electrónicas y permitiendo la colaboración directa con proveedores

de servicios en diferentes países y en situaciones de emergencia. También permite a los Estados Parte formar parte del Comité del Convenio sobre la Ciberdelincuencia para intercambiar información, evaluar la aplicación del Convenio y ofrecer orientación interpretativa. Esto fomenta la cooperación entre el sector privado y las autoridades de justicia penal. Además, los países que se adhieran pueden recibir asistencia técnica para mejorar su capacidad de cooperación internacional y aplicar plenamente el Convenio.

Por lo que la cooperación internacional en la lucha contra el delito informático requiere una visión global y conjunta, ejecutando políticas integradoras mediante una gobernanza global. Es crucial involucrar a todos los Estados y sectores de la sociedad en políticas conjuntas, priorizando convenios multilaterales sobre tratados bilaterales para armonizar las políticas regionales en cibercrímenes y lograr una regulación coherente a escala global, a pesar de los desafíos existentes en el entendimiento entre países y el entramado legislativo.

5. La Convención de las Naciones Unidas contra la Ciberdelincuencia (UNCC)

La Convención de las Naciones Unidas contra la Ciberdelincuencia (UNCC, por sus siglas en inglés y de ahora en adelante), aprobada mediante la Resolución A/RES/79/243[1], representa un hito normativo en el sistema multilateral al establecer un marco jurídico integral y universal para abordar el uso delictivo de las tecnologías de la información y la comunicación. A diferencia del Convenio de Budapest de 2001, que ha sido criticado por su enfoque eurocentrista y por haber sido negociado sin participación plena de muchos países en desarrollo, esta nueva Convención surge de un proceso intergubernamental abierto, inclusivo y universal, iniciado por la resolución 74/247 (2019) y continuado con la 75/282 (2021)[2], lo que le otorga una mayor legitimidad democrática en el seno de la ONU. Las cuales sentaron las bases para la elaboración de un instrumento jurídicamente vinculante capaz de responder a las amenazas que emergen del ciberespacio.

A través de la Resolución 74/247, se creó un comité intergubernamental especial con el mandato de elaborar una convención internacional sobre el uso delictivo de las tecnologías de la información y las comunicaciones (Asamblea General de las Naciones Unidas, 2024) tomando como base los esfuerzos nacionales, regionales e internacionales ya existentes.

En 2021, la Resolución 75/282 consolidó el mandato del Comité Especial, estableciendo su sede operativa entre Nueva York y Viena, con el objetivo de presentar un texto definitivo ante la Asamblea en su 78º período de sesiones (Asamblea General de las Naciones Unidas, 2024). Este proceso estuvo guiado por la necesidad de una cooperación internacional más robusta, especialmente ante la creciente sofisticación de los delitos cibernéticos y sus impactos negativos en el desarrollo sostenible, la seguridad global y el estado de derecho.

La resolución 79/243 reconoce explícitamente los desafíos contemporáneos derivados del uso indebido de las TIC y la disparidad en las capacidades estatales para hacerles frente (Asamblea General de las Naciones Unidas, 2024). Se manifiesta una clara intención de armonizar normas sustantivas y procesales en materia penal internacional, al tiempo que

[1] Resolución A/RES/79/243, adoptada el 24 de diciembre de 2024 por la Asamblea General de la ONU, disponible en: https://docs.un.org/es/A/RES/79/243

[2] Disponibles en: https://docs.un.org/es/A/Res/74/247 y https://docs.un.org/es/A/RES/75/282, respectivamente.

se fomenta el respeto a los derechos humanos, la soberanía estatal y la diversidad jurídica de los sistemas nacionales.

Con un proceso de negociación que se extendió por más de un lustro y que involucró no solo a los Estados Miembro, sino también a actores no estatales incluyendo organizaciones de la sociedad civil, el sector académico y empresas tecnológicas, el texto final refleja un delicado equilibrio entre intereses divergentes.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) asumió el rol de secretaría técnica durante las negociaciones, reforzando su papel central como órgano coordinador en la lucha global contra el crimen organizado (Asamblea General de las Naciones Unidas, 2024).

La Convención contra la Ciberdelincuencia ha sido abierta a firma en 2025, en Hanói, Vietnam, y entrará en vigor una vez que cuarenta Estados la ratifiquen (Asamblea General de las Naciones Unidas, 2024). Sin duda, esta convención representa un esfuerzo multilateral para enfrentar el uso indebido de las tecnologías de la información y la comunicación, cuya utilización delictiva se ha intensificado en escala, rapidez y alcance, superando las capacidades de respuesta tradicionales.

En el preámbulo y disposiciones iniciales, se reitera la urgencia de fortalecer la cooperación internacional frente a una amenaza cada vez más compleja y transfronteriza como lo es la ciberdelincuencia, destacando sus implicaciones negativas para la economía, el Estado de derecho y el desarrollo sostenible.

El Capítulo I, titulado Disposiciones Generales, introduce una aproximación renovada al tratamiento jurídico de los delitos cometidos mediante tecnologías digitales.

En dicho instrumento se proponen tres objetivos centrales establecidos en el art. 1 (Asamblea General de las Naciones Unidas, 2024):

1) Reforzar las medidas de prevención y combate a la ciberdelincuencia;
2) Fortalecer la cooperación internacional para hacer frente a este fenómeno;
3) Fomentar la asistencia técnica y el desarrollo de capacidades, con especial énfasis en el apoyo a los países en desarrollo.

A diferencia de la Convención de Budapest, que se enfoca predominantemente en delitos contra sistemas informáticos, la nueva Convención de las Naciones Unidas adopta un enfoque más amplio y transversal, al contemplar la utilización de las TIC en la comisión de delitos graves como el blanqueo de capitales, la corrupción, el terrorismo, la trata de personas, el tráfico ilícito de migrantes, armas, drogas y bienes culturales (Asamblea General de las Naciones Unidas, 2024). También destaca por incorporar con claridad la transmisión de pruebas electrónicas como un componente esencial de la cooperación penal internacional.

Los Capítulos III y IV de esta Convención representan un avance normativo significativo en la lucha contra la ciberdelincuencia, al establecer con mayor precisión y amplitud los criterios de jurisdicción y las medidas procesales que los Estados deben implementar para investigar y sancionar eficazmente estos delitos (Asamblea General de las Naciones Unidas, 2024). Reconociendo la complejidad propia del entorno digital, la normativa busca

equilibrar la necesidad de cooperación internacional y flexibilidad jurisdiccional con la protección de los derechos humanos.

Observamos que en el Capítulo III, dedicado a la jurisdicción, se amplían los supuestos que permiten a un Estado ejercer su competencia penal. Más allá del tradicional criterio territorial, la Convención contempla que la jurisdicción pueda extenderse a casos donde el delito afecte a nacionales, residentes o al propio Estado, incluso si la conducta se origina fuera de su territorio con la intención de causar un daño dentro de él (Asamblea General de las Naciones Unidas, 2024). Además, se promueve la coordinación entre Estados ante investigaciones simultáneas, lo cual contribuye a evitar duplicidades y conflictos, fortaleciendo la cooperación internacional.

Esta perspectiva supone una evolución frente al Convenio de Budapest de 2001, que adoptaba un enfoque más restrictivo, centrado en la jurisdicción territorial y la nacionalidad del autor, sin considerar expresamente escenarios transnacionales tan complejos ni mecanismos coordinados tan desarrollados. La nueva Convención responde así a las transformaciones tecnológicas y a la naturaleza global y descentralizada del cibercrimen, donde las fronteras tradicionales pierden eficacia para delimitar la acción delictiva.

Por su parte, el Capítulo IV aborda las medidas procesales y herramientas legales necesarias para la persecución penal en el ámbito digital. Se incorporan procedimientos detallados para la conservación acelerada de datos electrónicos, la emisión de órdenes para obtener información almacenada, la búsqueda e incautación de evidencia digital y la recolección en tiempo real tanto de datos de tráfico como de contenido de comunicaciones, Además, se destacan salvaguardas dirigidas a proteger los derechos fundamentales, como la proporcionalidad, la supervisión judicial y la confidencialidad, junto con medidas específicas para la protección de testigos y víctimas, lo que refleja un enfoque integral y respetuoso de los derechos humanos (Asamblea General de las Naciones Unidas, 2024).

En comparación con el Convenio de Budapest, que sentó las bases para la cooperación en ciberdelincuencia, pero ofrecía disposiciones menos detalladas en estas materias, esta Convención aporta una actualización y profundización importante. Destaca, además, el reforzamiento de los mecanismos para el embargo, incautación y decomiso de productos del delito, incluyendo la facultad para acceder a documentación bancaria y financiera, adaptándose mejor a la sofisticación de los delitos económicos y tecnológicos contemporáneos.

Lo cual evidencia un esfuerzo renovado por adecuar el marco jurídico internacional a las exigencias del ciberespacio actual, enfatizando una jurisdicción más flexible y una robusta capacidad procesal, sin perder de vista la protección de derechos fundamentales, lo que representa una respuesta más efectiva y contemporánea que el modelo planteado en Budapest en 2001.

Esta Convención se proyecta como un instrumento multilateral de segunda generación, con mayor alcance temático, legitimidad política e implicaciones normativas, especialmente para los países del Sur Global que hasta ahora habían tenido una participación limitada en los marcos existentes. Sin embargo, su efectividad dependerá de su implementación nacional, de los mecanismos de cooperación técnica que se establezcan y de su articulación con los principios del Derecho Internacional de los Derechos Humanos. De este

modo, se sientan las bases para una arquitectura jurídica internacional más robusta, adaptada a los desafíos complejos de la era digital.

Al posicionarse como instrumento global, este instrumento jurídico aspira a cerrar las brechas normativas, prevenir refugios seguros para ciberdelincuentes y garantizar un equilibrio entre eficacia penal y respeto a las garantías fundamentales en la era digital. No obstante, su implementación práctica enfrentará retos significativos. La eficacia del instrumento dependerá de la voluntad política de los Estados parte para armonizar sus marcos legales internos, asignar recursos suficientes y participar activamente en los mecanismos de cooperación internacional que establece. Sin esta articulación, las disposiciones del tratado corren el riesgo de quedarse en el plano declarativo.

La Convención de las Naciones Unidas contra la Ciberdelincuencia, adoptada en 2024, surge como un intento de establecer el primer instrumento multilateral de carácter verdaderamente global. A diferencia de Budapest, la UNCC fue negociada en el marco de la Asamblea General de la ONU, lo que le otorga mayor legitimidad política y cobertura potencial. Retoma elementos de convenios previos como Budapest y la Convención Árabe de 2010, pero introduce innovaciones relevantes:

1) *Jurisdicción ampliada*: incorpora el principio de personalidad pasiva, permitiendo a un Estado ejercer competencia cuando sus nacionales resulten afectados, incluso si el delito ocurrió en el extranjero.
2) *Mecanismos institucionales*: establece la Conferencia de los Estados Parte y una Secretaría permanente, algo que Budapest no contempla, para supervisar la implementación y coordinar con organismos como la UNODC.
3) *Salvaguardas jurídicas:* incluye cláusulas explícitas sobre proporcionalidad, revisión judicial independiente y prohibición de extradición en casos de persecución política, religiosa o de género, en un esfuerzo por balancear seguridad con derechos humanos.

No obstante, la UNCC también enfrenta críticas significativas. Algunos observadores advierten riesgos de vigilancia excesiva y censura, pues el tratado legitima la recolección de datos por parte de los Estados, aunque sujeta a controles legales. Asimismo, la cláusula de personalidad pasiva puede abrir la puerta a usos con motivaciones políticas, especialmente en países con instituciones débiles.

En términos comparativos, el Convenio de Budapest se caracteriza por su flexibilidad y por haber sentado las bases normativas regionales que inspiraron otros instrumentos. Sin embargo, su carácter eurocéntrico, las limitaciones temáticas y la ausencia de potencias tecnológicas restan eficacia a su alcance global. Por su parte, la UNCC representa un avance sustantivo hacia la universalización de un marco jurídico contra la ciberdelincuencia, con innovaciones procesales e institucionales que refuerzan la cooperación internacional. Aun así, su eficacia dependerá de la voluntad política de los Estados parte, de la aplicación efectiva de las salvaguardas y de su capacidad de evitar que se convierta en una herramienta de control estatal incompatible con la democracia y los derechos humanos.

En definitiva, ambas convenciones presentan fortalezas y limitaciones: Budapest, como referente técnico y precursor regional; la UNCC, como un esfuerzo multilateral más inclusivo y con vocación global. Su coexistencia marcará el futuro de la gobernanza global en

materia de ciberdelincuencia, donde la cooperación y la confianza mutua serán determinantes.

6. El caso de México

A más de dos décadas de la apertura a firma del Convenio de Budapest sobre la Ciberdelincuencia, México permanece como Estado observador, sin haber formalizado su adhesión. Esta omisión resulta particularmente significativa dada la creciente sofisticación y frecuencia de los delitos informáticos en el país, y evidencia un desfase normativo respecto de los estándares internacionales vigentes en la materia. A pesar de exhortos legislativos, como el emitido por el Senado en septiembre de 2021 (Ballinas y Becerril, 2021), el Poder Ejecutivo no ha formalizado la ratificación, lo que refleja una reticencia institucional que no puede entenderse como prudencia legislativa, sino como una manifestación de la debilidad estructural del sistema penal frente a los desafíos del entorno digital.

Desde una perspectiva jurídica, la resistencia mexicana se articula en torno a la tensión entre el derecho penal nacional y los compromisos que emanan del Derecho Internacional de los tratados. Conforme al Artículo 133 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM, por sus siglas y de ahora en adelante) los tratados internacionales ratificados por México tienen jerarquía equiparable a las leyes federales, lo que implica su aplicabilidad directa una vez publicados. Sin embargo, el orden constitucional también impone límites materiales: los Artículos 1 y 133 prohíben celebrar tratados que alteren los derechos humanos reconocidos por la propia Constitución, mientras que los Artículos 14 y 16 establecen el principio de legalidad penal, en su vertiente del *nullum crimen, nulla poena sine lege*.

Estos últimos consagran el principio de legalidad penal, lo que implica que ninguna persona puede ser sancionada sin que exista previamente una norma jurídica que tipifique de forma clara y específica la conducta sancionable. De este modo, se prohíbe constitucionalmente la imposición de penas que no se encuentren expresamente previstas en una ley vigente y aplicable al caso concreto.

La Suprema Corte de Justicia de la Nación (SCJN, por sus siglas y de ahora en adelante) ha sostenido que la descripción legal de un delito no puede ser vaga, ambigua ni sujeta a interpretaciones extensivas, ya que ello vulneraría la seguridad jurídica y abriría espacio a la arbitrariedad judicial[3]. En este sentido, ha enfatizado que los tipos penales deben contener "un contenido concreto y unívoco", estableciendo con claridad el bien jurídico tutelado, los elementos del tipo y los rangos punitivos correspondientes.

El Convenio de Budapest exige a los Estados Parte dos obligaciones fundamentales: primero, tipificar como delitos ciertas conductas relacionadas con el uso de tecnologías de la información, como el acceso ilícito a sistemas informáticos, la interceptación de datos, la alteración de información digital, la obstrucción de servicios, el abuso de dispositivos, la falsificación y el fraude informático, entre otros; y segundo, conferir a las autoridades judiciales y ministeriales poderes adecuados para investigar y sancionar tales delitos, incluyen-

[3] Ver: Tesis Jurisprudencial, 1a./J. 10/2006, Novena Época, Semanario Judicial de la Federación y su Gaceta. Tomo XXIII, marzo de 2006, p. 84.

do la vigilancia de comunicaciones, la recolección de datos de tránsito, el aseguramiento de evidencia digital y la colaboración transnacional.

En el caso mexicano, la incorporación de estas obligaciones no puede realizarse sin un proceso riguroso de armonización legislativa. Diversas disposiciones contenidas en el Convenio, particularmente los artículos 2 al 8, emplean conceptos como "ilegítimo" o "posesión" sin ofrecer una definición cerrada, lo que entra en fricción con el principio de legalidad penal en su dimensión de ley cierta y estricta. Por ejemplo, el artículo 2 sobre acceso ilícito y el artículo 6 sobre abuso de dispositivos, podrían interpretarse de manera tan amplia que habilitaran la persecución de conductas ambiguas, como el uso no autorizado de redes institucionales o la tenencia de herramientas informáticas utilizadas en pruebas de seguridad digital.

Además, la legislación penal mexicana no existe una sistematización suficiente en materia de ciberdelitos. El Código Penal Federal (CPF, por sus siglas y de ahora en adelante), si bien contempla algunas figuras delictivas relacionadas con la informática, lo hace de forma dispersa, sin un capítulo específico y sin tipificación integral. Esta fragmentación obstaculiza la aplicación homogénea de la ley y dificulta la capacitación de los operadores jurídicos. En este contexto, Danya Centeno (2018) ha propuesto la incorporación de un título específico sobre delitos informáticos en el CPF, lo que facilitaría la adecuación normativa al Convenio, garantizando claridad, coherencia y protección de derechos fundamentales.

Asimismo, debe considerarse la aplicación del principio de culpabilidad, que implica que la imposición de penas sólo puede realizarse sobre la base de hechos concretos imputables al sujeto, y no sobre su personalidad o supuesta peligrosidad. La ambigüedad de los tipos penales previstos en el Convenio podría derivar en un uso punitivo desproporcionado, especialmente en un contexto como el mexicano, donde se ha documentado el uso arbitrario de tecnologías de vigilancia por parte de autoridades estatales.

La no ratificación del Convenio de Budapest por parte de México no puede ser atribuida únicamente a una omisión política. Se trata de una decisión que evidencia tensiones estructurales entre el derecho penal nacional y los compromisos internacionales, y que requiere una estrategia legislativa articulada para asegurar que la adhesión al tratado no vulnere principios constitucionales ni habilite el uso discrecional del poder punitivo del Estado. Mientras no se subsanen las deficiencias normativas internas y se establezca un marco penal técnica y constitucionalmente compatible con los estándares del Convenio, su ratificación resultará no solo inviable, sino también riesgosa desde el punto de vista de los derechos fundamentales.

A más de dos décadas de su adopción, el Convenio Budapest permanece sin ratificación por parte de México, a pesar de los crecientes riesgos estructurales que enfrenta el país en el entorno del ciberespacio y de los múltiples llamados institucionales para revisar su estatus jurídico. En septiembre de 2021, el Senado mexicano exhortó al Poder Ejecutivo a concluir la evaluación de dicho instrumento, subrayando su importancia para articular una política criminal eficaz en el ciberespacio (Ballinas y Becerril, 2021). Sin embargo, la postura de México no necesariamente obedece a una postura estratégica deliberada, sino que más bien revela una tensión estructural persistente entre la necesidad de armonizar el marco jurídico nacional con los estándares internacionales y las restricciones constitucio-

nales que rigen el derecho penal interno. Esta ambivalencia ilustra los dilemas normativos que enfrenta el país ante la expansión de una criminalidad transnacional cuya naturaleza digital exige respuestas jurídicas igualmente transfronterizas.

Dicho Convenio establece que los Estados parte deben adoptar medidas legislativas, administrativas y de otra índole que les permitan tipificar penalmente, dentro de su jurisdicción, una serie de conductas relacionadas con los sistemas informáticos. Estas conductas abarcan:

- El acceso intencional y no autorizado, total o parcial, a un sistema informático (Artículo 2).
- La interceptación deliberada e ilegítima, mediante herramientas técnicas, de datos transmitidos en comunicaciones no públicas dentro de un sistema informático (Artículo 3).
- Las afectaciones a la integridad de los datos, como su alteración, supresión, deterioro o eliminación de forma deliberada y sin autorización (Artículo 4).
- La interferencia intencional y no autorizada que cause una interrupción significativa en el funcionamiento de un sistema informático (Artículo 5).
- La creación, adquisición, distribución o cualquier forma de facilitación de herramientas –incluyendo software, dispositivos o contraseñas– destinadas a la comisión de los delitos anteriores (Artículo 6).
- Otros delitos como la falsificación informática, el fraude informático, la pornografía infantil y las infracciones a los derechos de propiedad intelectual o derechos afines (Artículos 7 a 10).

Estas disposiciones reflejan no solo un esfuerzo por establecer un lenguaje penal común frente a las amenazas cibernéticas sino también un intento de fomentar la cooperación internacional y la asistencia jurídica mutua entre los Estados. Empero, la adhesión plena al Convenio implica también un ejercicio complejo de adecuación normativa que, en el caso mexicano, se enfrenta al reto de armonizar las disposiciones internacionales con el principio de legalidad penal, los límites al ius puniendi y la protección de los derechos fundamentales previstos en la Constitución.

Es decir, este rezago se torna más apremiante cuando se consideran los efectos jurídicos de la eventual ratificación. Conforme al artículo 133 de la CPEUM, los tratados internacionales válidamente celebrados por el Estado mexicano forman parte del derecho interno. Ello implicaría que, una vez ratificado, el Convenio de Budapest tendría eficacia directa y vinculante para jueces y autoridades nacionales. No obstante, esta aparente ventaja jurídica plantea complejidades de compatibilidad si se analiza a la luz del principio de legalidad penal consagrado en los artículos 14 y 16 constitucionales, que exige una definición precisa, clara y estricta de los tipos penales.

En este sentido, el Convenio de Budapest presenta ambigüedades sustanciales en la redacción de algunas de sus figuras típicas como el acceso ilícito, la interceptación ilegal o el uso indebido de dispositivos al utilizar expresiones genéricas como "sin derecho", "de forma ilegítima" o "con fines delictivos" sin especificar el bien jurídico protegido o los límites objetivos de la conducta punible. Este tipo de formulaciones abiertas, si bien útiles para sistemas de derecho anglosajón o mixto, entra en tensión con la tradición penal garantista

del ordenamiento mexicano, que exige una taxatividad absoluta en la formulación normativa para evitar tanto la impunidad como la discrecionalidad punitiva (Centeno, 2018).

El debate, por tanto, no se limita a lo técnico, sino que implica una tensión estructural entre la apertura internacional del derecho penal y los límites de un constitucionalismo mexicano. Este vacío normativo contrasta con la realidad de vulnerabilidad digital que enfrenta el Estado mexicano. En los últimos años, el país ha sido blanco de ciberataques de alto impacto, incluyendo incidentes dirigidos contra infraestructuras críticas como PEMEX (la petrolera estatal), el IMSS (seguridad social), la Secretaría de Economía o la propia Secretaría de la Defensa Nacional. La sofisticación de los ataques que van desde campañas de *ransomware* hasta intrusiones persistentes avanzadas evidencia que la falta de adhesión al Convenio de Budapest no es una simple omisión diplomática, sino una renuncia táctica a construir un marco normativo de respuesta articulada frente a amenazas transnacionales.

La adhesión de México requerirá una reingeniería normativa orientada a garantizar compatibilidad entre el tratado y los principios rectores del derecho penal nacional. En términos legislativos, dos rutas se perfilan como posibles: la creación de una ley especial en materia de delitos informáticos, o bien la modificación sustancial del Código Penal Federal para incorporar los tipos penales previstos en el Convenio. Si bien la primera opción puede ofrecer ventajas pedagógicas y especialización técnica, su implementación efectiva sería limitada en un sistema caracterizado por la falta de articulación normativa, escasa capacitación judicial y reducida interoperabilidad institucional. Por el contrario, una reforma integral al CPF permitiría una inserción orgánica del Convenio en el marco penal vigente, evitando duplicidades normativas y asegurando coherencia entre los principios sustantivos y las reglas de imputación penal (Centeno, 2018).

La ciberseguridad enfrenta importantes retos estructurales, derivados de la ausencia de un marco legal integral y de la fragmentación regulatoria entre múltiples agencias. Aunque instituciones como la Fiscalía General de la República, la CNBV, el Banco de México, el INAI y la Guardia Nacional desempeñan funciones específicas en la protección del ciberespacio, la falta de coordinación y estandarización de políticas limita la eficacia de las acciones preventivas y reactivas frente a incidentes cibernéticos. Este panorama resalta la necesidad de fortalecer la gobernanza institucional, promover la cooperación interinstitucional y desarrollar un marco normativo integral, que permita a México enfrentar de manera más sólida las amenazas cibernéticas y garantizar la protección de la infraestructura crítica y los derechos digitales de la ciudadanía (Vela-Treviño y Villanueva-Plasencia, 2025).

En el ámbito internacional, ha reafirmado su compromiso con la cooperación y actualización del marco normativo para enfrentar delitos cibernéticos, proteger datos personales y garantizar derechos humanos (Salas, 2025), a través de la celebración de la Convención de las Naciones Unidas contra la Ciberdelincuencia en diciembre de 2024 en Hanoi, Vietnam, aunque aún no la ha ratificado. Este acto refuerza dicho compromiso, mientras que las cifras del Reporte Global de Amenazas 2025, que registran 35,200 millones de intentos de ciberataques en los primeros tres meses del año, posicionan a México como el segundo país más afectado de la región y evidencian la urgencia de implementar políticas robustas de ciberseguridad (Salas, 2025).

De tal forma que el verdadero desafío no radica en firmar el tratado, sino en transformar el sistema jurídico interno para responder con legalidad, proporcionalidad y eficacia a las amenazas digitales del siglo XXI. Solo así podrá el Estado mexicano avanzar hacia una soberanía digital robusta, que conjugue seguridad, cooperación internacional y protección efectiva de los derechos humanos en el entorno digital.

7. Hacia una gobernanza híbrida para la ciberseguridad y la justicia digital

En correspondencia con lo anteriormente expuesto, ni Budapest ni la Convención de la ONU, por sí solos, pueden resolver la complejidad del ecosistema cibernético actual. Por ello, se propone avanzar hacia un modelo de gobernanza híbrida, que integre:

- interoperabilidad técnica entre instrumentos,
- salvaguardas estrictas de derechos humanos,
- cooperación operativa ágil y multilateral,
- mecanismos inclusivos que reduzcan asimetrías geopolíticas,
- fortalecimiento de capacidades en países con pocos recursos,
- participación activa del sector privado, la academia y la sociedad civil.

Este modelo permitiría armonizar el enfoque tecnonormativo del Consejo de Europa con la búsqueda de legitimidad global y justicia digital impulsada desde la ONU. La ciberseguridad, entendida no solo como protección técnica sino como condición para el ejercicio de derechos y la cohesión democrática, requiere de una arquitectura de gobernanza compleja, adaptativa y cooperativa.

Sin ello, el ciberespacio corre el riesgo de consolidarse como un ámbito de impunidad estructural, donde las brechas regulatorias erosionen los cimientos del derecho internacional contemporáneo.

8. Conclusiones

La comparación entre el Convenio de Budapest y la propuesta de Convención de la ONU revela que ambos instrumentos responden a lógicas normativas y políticas distintas, pero potencialmente complementarias. Mientras el primero privilegia la estandarización técnico-jurídica y la eficiencia operativa, el segundo busca articular un marco verdaderamente universal que incorpore principios de derechos humanos, soberanía digital y gobernanza inclusiva. Esta divergencia no solo refleja diferencias en capacidades estatales o prioridades nacionales, sino también las tensiones geopolíticas que estructuran el orden digital contemporáneo.

Si bien el Convenio de Budapest aporta una base probada y ampliamente implementada cuya eficacia práctica constituye una ventaja difícil de ignorar sus limitaciones respecto de legitimidad global, diversidad de modelos regulatorios y sensibilidad a desigualdades estructurales resultan cada vez más evidentes. Por otro lado, la Convención de la ONU, aun con su ambición normativa y su potencial democratizador, enfrenta riesgos de fragmentación política, estancamiento negociador y posibles usos indebidos por parte de regímenes autoritarios.

Ante este escenario, la solución no pasa por elegir entre uno u otro modelo, sino por avanzar hacia un esquema de gobernanza digital híbrido y pragmático. Tal enfoque implica:

- promover la interoperabilidad técnica sin sacrificar garantías de derechos,
- fortalecer mecanismos de cooperación multinivel que reduzcan las brechas de capacidad entre Estados;
- asegurar procesos de gobernanza más inclusivos, con participación significativa del Sur Global, de la sociedad civil y de actores técnicos;
- y consolidar salvaguardas que prevengan la instrumentalización política de la normativa penal.

México se encuentra en un momento decisivo: avanzar hacia un marco integral de ciberseguridad no solo implica establecer regulaciones y agencias, sino también consolidar una visión estratégica, multidimensional y prospectiva, que posicione al país con capacidad de respuesta frente a los desafíos del ciberespacio.

Referencias

Ballinas, V., y Becerril, A. (2021, 15 de septiembre). Urgen a que México firme el Convenio de Budapest. *La Jornada*: https://www.jornada.com.mx/notas/2021/09/15/politica/urgen-a-que-mexico-firme-el-convenio-de-budapest/

Bartolomé, M. (2020). *Ciberseguridad: retos y perspectivas en el ámbito global*. Instituto Español de Estudios Estratégicos: https://www.ieee.es

Centeno, D. (2018). *México y el Convenio de Budapest: posibles incompatibilidades*. Red en Defensa de los Derechos Digitales / Derechos Digitales.

Chang, A. (2014). "China's cybersecurity strategy". Center for a New American Security. Disponible en: http://www.jstor.com/stable/resrep06327

Consejo de Europa. (2001). "Convenio sobre la Ciberdelincuencia" (Convenio de Budapest), disponible en: https://www.coe.int

CrowdStrike. (2024). Global Threat Report 2024. CrowdStrike Inc.: https://www.crowdstrike.com

Dunn Cavelty, M., y Wenger, A. (2019). *Cyber security politics: Socio-technological transformations and political fragmentation*. Routledge.

Fondo Monetario Internacional. (2024). Informe sobre la estabilidad financiera mundial: abril de 2024, disponible en: https://www.imf.org

Gutiérrez, E. (2020). "La responsabilidad internacional por el uso de la fuerza en el ciberespacio". Aranzadi.

Ibáñez, J. (2002), "Poder y autoridad en las relaciones internacionales: el control del comercio electrónico" [tesis de doctorado, Universitat Pompeu Fabra]. Tesis Doctorals en Xarxa. Disponible en: https://www.tdx.cat/handle/10803/7281#page=1

Ibarra, J., y Nieves, J. (2016). "La seguridad cibernética en el sistema interamericano: avances y desafíos". Organización de los Estados Americanos – CICTE.

Naciones Unidas. (2022–2024). A/RES/74/247: Elaboración de una convención integral sobre la lucha contra el uso de las TIC con fines delictivos.

Oficina del FBI. (1990). "Operation Sun Devil". U.S. Department of Justice.

OGDI. Observatorio de Delitos Informáticos. (2016). "Historia del cibercrimen y cooperación internacional".

Organización de Estados Americanos. (2002). Declaración sobre Seguridad en las Américas (Declaración de Bridgetown). OEA.

Organización de Estados Americanos. (2003). Conferencia Especial sobre Seguridad: Declaración de México. OEA, disponible en: https://www.oas.org

Piñón, R. (2018). "La gobernanza global, la seguridad internacional y la Unión Europea amenazadas por un mundo convulso". Centro de Estudios Latinoamericanos Facultad de Ciencias Políticas y Sociales UNAM: https://doi.org/10.22201/cela.24484946e.2018.41.64146

Robles, J. (2016). *Ciberseguridad y Derecho Internacional: soberanía, jurisdicción y atribución de responsabilidad*. Instituto Matías Romero.

Sain, M. (2015). *Cibercrimen y globalización económica: riesgos y desafíos*. Universidad de La Plata.

Sain, M. (2018). "Historia del delito informático: de los telégrafos al hacking moderno". *Revista de Estudios sobre Seguridad*.

Salas, C. (2025, 27 agosto). "México y la ONU refuerzan alianzas para enfrentar ciberdelitos y fortalecer la ciberseguridad en Iberoamérica". *Infobae*: https://www.infobae.com/mexico/2025/08/27/mexico-y-la-onu-refuerzan-alianzas-para-enfrentar-ciberdelitos-y-fortalecer-la-ciberseguridad-en-iberoamerica/

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Ülgen, S. (2016). "Cybersecurity" en: *Governing cyberspace: A Road Map for Transatlantic Leadership*. Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep26924.11

Vela-Treviño, C., y Villanueva-Plasencia, D. (2025, enero 7). *Cybersecurity in Mexico: A comprehensive overview*. Baker McKenzie Connect on Tech, en: https://connectontech.bakermckenzie.com/cybersecurity-in-mexico-a-comprehensive-overview/

Vila, M. y Saguier, M. (2019). "Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional". *Revista de Relaciones Internacionales*, n.° 40, 113–131: https://revistas.uam.es/relacionesinternacionales/article/download/relacionesinternacionales2019_40_005/10824/25587

Zunzunegui, S. (2008). "Delitos informáticos y jurisdicción internacional: retos del cibercrimen". *Revista de Derecho y Tecnología*, 12, 165–184.