Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

05.07.2024

Informe Final de Recomendaciones del Knowmad Institut sobre la Convención de Cibercrimen de la ONU (Mayo 2024)

COMENTARIOS FINALES Y RECOMENDACIONES AL COMITÉ AD HOC ENCARGADO DE ELABORAR UNA CONVENCIÓN INTERNACIONAL COMPRENSIVA SOBRE LA LUCHA CONTRA EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES CON FINES DELICTIVOS, SOBRE EL TEXTO ACTUALIZADO DE LA CONVENCIÓN CON FECHA DE MAYO DE 2024.

European Institute for Multidisciplinary Studies on Human Rights and Sciences - Knowmad Institut.

Grupo Especial de Trabajo:
Ob. Martin Ignacio Díaz Velásquez, Prof. Jorge Vicente Paladines, Dra. Leticia Fuentes Vera, Ing. Jesús Alfredo Ribero Faria, MSc. Oscar Hugo Espin García, Rev. Daniela Kreher, MSc. Ludwing Moncada Bellorin.

INTRODUCCIÓN

El **Knowmad Institut - Instituto Europeo de Estudios Multidisciplinarios Sobre Derechos Humanos y Ciencias**, comprometido con la promoción de la dignidad humana y el desarrollo sostenible, presenta los siguientes comentarios y recomendaciones para el texto actualizado de la **Convención Internacional Sobre La Lucha Contra El Uso De Las Tecnologías De La De La Información Y Las Comunicaciones Con Fines Delictivos (*A/AC.291/22/Rev.3*)**. Estas recomendaciones se basan en un análisis detallado del borrador del convenio, los documentos complementarios con referencias *A/AC.291/25/Rev.1* y *A/AC.291/27* y las contribuciones previas del Knowmad Institut a este distinguido comité (***Recs. 3ra Sesión***; ***Recs. 4ta Sesión***). Nuestro enfoque se centra en asegurar que la convención proteja los derechos y la dignidad humana, que promueva la cooperación internacional y adopte un enfoque equilibrado y eficaz para combatir el cibercrimen.

Nota: Este documento es una versión resumida de nuestro análisis y comentarios detallados que se pueden encontrar aquí.

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

PREÁMBULO

El Knowmad Institut, conocido por su enfoque multidisciplinario en los estudios de derechos humanos y ciencias, ha participado activamente en las sesiones previas del Comité Ad Hoc para la elaboración de un convenio internacional integral contra el uso criminal de las tecnologías de la información y la comunicación (TIC). En nuestras contribuciones anteriores, destacamos la importancia de un enfoque equilibrado y comprensivo que respete el derecho al anonimato y la protección de datos personales para crear espacios seguros en el ciberespacio. Además, subrayamos la necesidad de que la promoción y protección de los derechos humanos sean los objetivos primarios al regular las TIC, asegurando que el acceso a la tecnología mejore la calidad de vida sin infringir derechos y libertades.

Propusimos la inclusión de una cláusula específica para proteger a grupos vulnerables y priorizar la representación inclusiva de personas expuestas a conflictos o persecuciones de naturaleza política, étnica, religiosa o por origen migratorio. Además, enfatizamos la necesidad de adoptar un enfoque interseccional de derechos humanos con perspectiva de género y la relevancia de la ciencia abierta como herramienta para prevenir el uso criminal de las tecnologías de la información y la comunicación (TIC). Consideramos especialmente urgente abordar las amenazas potenciales de persecución debido al origen migratorio, reconociendo que la diversidad de dialectos, especialmente en regiones del sur global, puede ser erróneamente interpretada como un método de "encriptación" de posibles mensajes criminales. Esta perspectiva es esencial para fortalecer la cooperación internacional en la prevención de ciberdelitos y delitos híbridos, así como en la intercepción de telecomunicaciones, garantizando un enfoque inclusivo y no discriminatorio en la prevención del crimen.

Remarcamos la preocupación colectiva por los desafíos que plantean los servicios de espionaje externalizados y la recolección de inteligencia, destacando la necesidad de una regulación y supervisión rigurosas para proteger la integridad física de individuos de la sociedad civil organizada en particular y de la sociedad en general. Además, abordamos la problemática del tráfico de sustancias controladas a través del internet y su impacto en la salud pública, sugiriendo estrategias de reducción de daños y deflexión para mitigar los efectos negativos en la comunidad.

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

RECOMENDACIONES

Nuestras recomendaciones y comentarios sobre el borrador de la convención con identificador: ***A/AC.291/22/Rev.3*** enfatizan la protección de derechos humanos y la privacidad, alineándose con estándares internacionales como el Pacto Internacional de Derechos Civiles y Políticos. Se destaca la importancia de actualizar y clarificar definiciones sobre tecnologías emergentes para garantizar una regulación efectiva y adaptativa.

Se propone la incorporación de mecanismos independientes de supervisión y evaluación que involucren a la sociedad civil, asegurando que las medidas adoptadas sean justas y respeten los derechos humanos. Además, se recomienda implementar programas educativos y preventivos para aumentar la conciencia sobre la seguridad en las TIC y mitigar los riesgos asociados al cibercrimen.

Se aconseja definir claramente las acciones que constituyen delitos en el ámbito digital y establecer sanciones proporcionales que sean disuasorias y ajustadas a la gravedad de los delitos. También se sugiere proteger de manera especial a los menores de edad y promover la cooperación internacional para combatir el abuso infantil en línea.

Se enfatiza la necesidad de fomentar la cooperación internacional y la armonización de leyes para una respuesta coordinada y efectiva contra los ciberdelitos. Esto incluye clarificar la jurisdicción y mejorar los procedimientos legales para facilitar investigaciones y enjuiciamientos eficaces.

Las recomendaciones también abordan la importancia de proteger los datos personales durante las transferencias internacionales y establecer normativas claras para la extradición que respeten los derechos humanos. Una vez utilizados los datos personales, dependiendo del caso, se deben eliminar. Además, se recomienda facilitar la transferencia de procedimientos penales y mejorar la asistencia legal mutua entre estados para fortalecer la lucha contra el cibercrimen a nivel global.

Adicionalmente, se subraya la necesidad de crear y fortalecer las leyes en los Estados Parte para que protejan a testigos y denunciantes de represalias, incluyendo la intimidación y el acoso. Para esto, se deben establecer programas de protección de testigos, que incluyan medidas específicas como la protección física o la reubicación, así como mecanismos para la no divulgación de información sobre la identidad y el paradero de los testigos.

DOI: 10.5281/zenodo.12668116

En este sentido, se propone aplicar las medidas de protección tanto a las víctimas como a testigos, proporcionando apoyo psicológico y legal para que puedan testificar sin riesgo de represalias. También se sugiere dar seguimiento a estos testigos y denunciantes de cibercrímenes para asegurar la efectividad de las medidas de protección.

Por último, se recomienda adoptar normas internacionales, como las de la Convención de Budapest, para alinear estándares y facilitar la cooperación global. Esto incluye la consulta con expertos y partes interesadas para recomendar reformas sólidas con definiciones claras que garanticen la proporcionalidad de la pena, así como el fortalecimiento de la infraestructura tecnológica para detectar el cibercrimen y responder eficazmente. Capacitar a jueces, fiscales y fuerzas del orden es esencial para garantizar el manejo adecuado de los delitos cometidos en el ciberespacio o de manera híbrida dentro del sistema judicial. Las campañas de sensibilización pública pueden ayudar a prevenir estos delitos al informar a la ciudadanía sobre los riesgos y las medidas de protección.

En breve, nuestras recomendaciones buscan establecer un marco robusto y respetuoso con los derechos y la dignidad humana que permita prevenir y perseguir el cibercrimen de manera efectiva, mientras se protege la integridad y la privacidad de los individuos en el entorno digital. La implementación de estas medidas promoverá una cooperación internacional equilibrada y efectiva, garantizando al mismo tiempo la dignidad humana y el desarrollo sostenible.

RECOMENDACIONES TEMÁTICAS

Protección de Derechos Humanos y Privacidad

- **Incorporación en Artículos:** Artículo 1, Artículo 6.
- **Detalle:** Asegurar que todas las medidas adoptadas respeten los derechos humanos y la privacidad, refiriéndose explícitamente a marcos de derechos humanos existentes, como el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) (Naciones Unidas, 1966). Este enfoque protege las libertades fundamentales y refuerza la legitimidad de las acciones contra el cibercrimen (Meier et al., 2020; Ali et al., 2022; Montal & Pauselli, 2023; Ajoy, 2022; Da-Yu Kao et al., 2019; Feldle, 2020; Kennedy & Warren, 2020; Ahsan et al., 2022).

DOI: 10.5281/zenodo.12668116

Definiciones Claras y Actualizadas

- **Incorporación en Artículos:** Artículo 2, Artículo 3.
- **Detalle:** Incluir definiciones adicionales que reflejen tecnologías emergentes como la Inteligencia Artificial, el Internet de las Cosas (IoT) y blockchain. Establecer un mecanismo para la revisión y actualización periódica de las definiciones para asegurar su relevancia continua (Weber, 2009; Lobach et al., 2021; Aulia, 2023; Han, 2023; Klevtsov, 2020; Varshney et al., 2020; Balajanov, 2018).

Medidas de Supervisión y Evaluación

- **Incorporación en Artículos:** Artículo 6, Artículo 24.
- **Detalle:** Establecer mecanismos independientes de supervisión y evaluación para asegurar que las medidas adoptadas bajo la convención se alineen con los estándares internacionales de derechos humanos. Es ampliamente recomendable la creación de comités de supervisión y la participación de organizaciones de la sociedad civil y otras partes interesadas (Cross, 2017; Curtis & Oxburgh, 2023; Holt, 2018; Mantovani, 2020; Nurahman, 2019; Brenner & Clarke, 2009).

Medidas Preventivas y Educativas

- **Incorporación en Artículos:** Artículo 7, Artículo 8, Artículo 9, Artículo 11.
- **Detalle:** Además de la criminalización, incluir disposiciones sobre medidas preventivas y programas educativos para concienciar a la sociedad sobre la importancia de la seguridad en las TIC y prevenir incidentes de cibercrimen (Krastev, 2022; ECPAT International, 2016; Gunarto et al., 2023; Grauer, 2022; Saxena, 2023; Cerezo et al., 2007; Kagita et al., 2020).

Clarificación de Alcances y Sanciones

- **Incorporación en Artículos:** Artículo 10, Artículo 12, Artículo 13.
- **Detalle:** Definir claramente qué constituye interferencia y falsificación en el contexto de datos y sistemas electrónicos. Establecer sanciones proporcionales y efectivas, adaptadas a la gravedad del delito, y asegurar que las sanciones sean disuasorias y justas (Aldridge et al., 2017; Ajoy, 2022; Kaur, 2021; Sabu et al., 2023; Sprott, 2006; Khan et al., 2022).

DOI: 10.5281/zenodo.12668116

Protección de Menores y Medidas Especiales

- **Incorporación en Artículos:** Artículo 14, Artículo 15, Artículo 16.
- **Detalle:** Definir claramente "material de abuso sexual infantil", "solicitud," y "acoso" es crucial para evitar interpretaciones ambiguas que puedan resultar en lagunas legales y la falta de protección efectiva para los menores. Incluir mecanismos coordinados de apoyo y rehabilitación para las víctimas, y promover la cooperación internacional para la prevención y persecución del abuso sexual infantil en línea (Interpol, 2022; Bunga & Hiariej, 2019; Henry et al., 2020; Irawan et al., 2022; Citron & Franks, 2014; Knowmad Institut, 2023).

Cooperación Internacional y Armonización de Leyes

- **Incorporación en Artículos:** Artículo 17, Artículo 18, Artículo 19, Artículo 22, Artículo 23.
- **Detalle:** Fomentar la cooperación internacional y la armonización de leyes entre los Estados Parte para asegurar una respuesta coordinada y efectiva a los ciberdelitos. Establecer mecanismos claros de coordinación y colaboración (Broadhurst, 2017; Skulysh, 2014; Wingfield & Wingo, 2021; Dragomir, 2022; McGlynn & Rackley, 2017; Mabeka & Cassim, 2023).

Jurisdicción y Aplicación de Leyes

- **Incorporación en Artículos:** Artículo 19, Artículo 21, Artículo 24, Artículo 25.
- **Detalle:** Asegurar que los Estados Parte definan claramente los límites y alcances de su jurisdicción sobre los delitos cibernéticos y adopten medidas legislativas que permitan la implementación efectiva de los poderes y procedimientos necesarios para las investigaciones y enjuiciamientos (Hursevich, 2019; PTACC, 2022; Nurahman, 2020; Ruslan, 2023; Wilson, 2008; Setiawahyudi, 2015; Snail, 2009; Szongoth & Vetter, 2018; Teichmann & Wittmann, 2022; Tiutiuhin, 2022; Veresha, 2018; Voynova, 2015; Wicki-Birchler, 2020).

Preservación y Divulgación Parcial de Datos de Tráfico

- **Incorporación en Artículos:** Artículo 26.
- **Detalle:** Asegurar la conservación expedita de datos de tráfico, incluso cuando múltiples proveedores de servicios estén involucrados. Implementar procedimientos claros para la divulgación rápida de datos de tráfico a las autoridades competentes.

DOI: 10.5281/zenodo.12668116

La convención podría especificar los plazos y las condiciones bajo las cuales los proveedores de servicios deben proporcionar estos datos (Wicki-Birchler, 2020; Saxena, 2023).

Orden de Producción

- **Incorporación en Artículos:** Artículo 27.
- **Detalle:** Adoptar medidas legislativas claras que especifiquen los procedimientos y requisitos para emitir órdenes de producción. Incluir salvaguardas adecuadas para proteger la privacidad y los derechos de los individuos cuando se emiten órdenes de producción. Fomentar la colaboración transparente entre las autoridades competentes y los proveedores de servicios para con los usuarios (Curtis & Oxburgh, 2023; Wicki-Birchler, 2020; Saxena, 2023).

Búsqueda e Incautación de Datos Electrónicos Almacenados
Recolección en Tiempo Real de Datos

- **Incorporación en Artículos:** Artículo 28. Artículo 29.
- **Detalle:** Especificar los procedimientos para el registro e incautación de datos electrónicos y de la recolección en tiempo real de datos, asegurando que las autoridades competentes puedan actuar de manera eficiente y dentro del marco legal establecido. Incluir disposiciones para mantener la integridad y seguridad de los datos electrónicos durante y después de su recolección o incautación. Fomentar la colaboración con expertos en tecnologías de la información, telecomunicaciones y ética (Curtis & Oxburgh, 2023; Feldle, 2020; Da-Yu Kao et al., 2019; Wicki-Birchler, 2020; Saxena, 2023).

Intercepción de Datos de Contenido

- **Incorporación en Artículos:** Artículo 30.
- **Detalle:** Especificar los procedimientos y requisitos para la intercepción de datos de contenido, asegurando que las autoridades competentes puedan actuar de manera eficiente y dentro del marco legal establecido. Obligar a los proveedores de servicios a cooperar plenamente con las autoridades competentes y a mantener la capacidad técnica para interceptar y registrar datos de contenido en tiempo real. Incluir disposiciones para garantizar la confidencialidad de la intercepción de datos de contenido (Clough, 2015; Han, 2023; Sabu et al., 2023).

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

Congelación, Incautación y Confiscación de los Ingresos de Crimen

- **Incorporación en Artículos:** Artículo 31.
- **Detalle:** Implementar medidas legislativas claras que permitan la confiscación de productos del delito y de los bienes utilizados en la comisión de ciberdelitos. Asegurar que las autoridades tengan las herramientas legales y técnicas necesarias para identificar, rastrear y congelar bienes relacionados con ciberdelitos. Establecer procedimientos claros para la administración de bienes congelados, incautados o confiscados (Setiawahyudi, 2015; Snail, 2009; Rajaan & Dadhich, 2020).

Establecimiento de un Registro Criminal

- **Incorporación en Artículos:** Artículo 32.
- **Detalle:** Adoptar medidas legislativas que permitan la consideración de condenas previas de otros Estados en los procedimientos penales nacionales. Establecer mecanismos de cooperación internacional que faciliten el intercambio de información sobre condenas previas entre Estados. Incluir salvaguardas para proteger los derechos del acusado (Tiutiuhin, 2022; Sprott, 2006; Papai-Tarr, 2020).

Protección de Testigos

- **Incorporación en Artículos:** Artículo 33.
- **Detalle:** Crear y fortalecer las leyes para proteger a testigos y denunciantes de represalias, incluyendo la intimidación y el acoso. Establecer medidas específicas como la protección física o la reubicación, y crear mecanismos para la no divulgación de información sobre la identidad y el paradero de los testigos. Aplicar las medidas de protección tanto a las víctimas como a testigos y proveer apoyo psicológico y legal (Sarkar & Shukla, 2023; Nurahman, 2020).

Asistencia y Protección a Víctimas

- **Incorporación en Artículos:** Artículo 34.
- **Detalle:** Implementar medidas legislativas que garanticen la asistencia y protección de las víctimas de delitos cibernéticos, incluyendo mecanismos de apoyo psicológico y físico. Establecer procedimientos claros para que las víctimas puedan obtener compensación y restitución. Incluir las opiniones y preocupaciones de las víctimas en los procedimientos penales (Mabeka & Cassim, 2023; Agung et al., 2023; Veresha, 2018).

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

Principios Generales de Cooperación Internacional

- **Incorporación en Artículos:** Artículo 35.
- **Detalle:** Fortalecer los mecanismos de cooperación internacional, asegurando que existan protocolos claros y efectivos para la colaboración en investigaciones de cibercrimen. Armonizar las legislaciones nacionales con las normas internacionales (Klevtsov, 2020; Cerezo et al., 2007; Skulysh, 2014).

Protección de Datos Personales

- **Incorporación en Artículos:** Artículo 36.
- **Detalle:** Adoptar medidas legislativas claras que regulen la transferencia de datos personales conforme a las leyes nacionales e internacionales. Establecer acuerdos bilaterales o multilaterales que faciliten la transferencia segura de datos personales. Asegurar que los datos personales recibidos estén sujetos a salvaguardias efectivas y apropiadas (Gulczyńska, 2021; Mantovani, 2020; Buković, 2020).

Transferencia de Procedimientos Penales

- **Incorporación en Artículos:** Artículo 39.
- **Detalle:** Adoptar medidas legislativas que faciliten la transferencia de procedimientos penales. Establecer acuerdos bilaterales o multilaterales para facilitar la transferencia de procedimientos penales que respeten los derechos humanos de los acusados (Voynova, 2015; Klevtsov, 2020; Hursevich, 2019).

Principios Generales y Procedimientos Relacionados con la Asistencia Legal Mutua

- **Incorporación en Artículos:** Artículo 40.
- **Detalle:** Adoptar medidas legislativas y procedimientos claros que faciliten la asistencia legal mutua en investigaciones de cibercrimen. Fomentar la colaboración internacional mediante acuerdos bilaterales y multilaterales. Asegurar que los procedimientos de asistencia legal mutua respeten los derechos humanos de todas las partes involucradas (Hunton, 2012; Wilson, 2008; Mabeka & Cassim, 2023).

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

CONSIDERACIONES FINALES

El Knowmad Institut insta al Comité Ad Hoc a considerar estas recomendaciones para asegurar que la convención propuesta no solo sea eficaz en la lucha contra el cibercrimen, sino que también respete y proteja los derechos humanos y las libertades fundamentales. La implementación de estas recomendaciones promoverá una cooperación internacional equilibrada y efectiva, garantizando al mismo tiempo la dignidad humana y el desarrollo sostenible.

Además, es imperativo que la convención considere y mitigue cualquier potencial uso indebido de las tecnologías de vigilancia. Nos preocupa que el enfoque de la convención pueda ser interpretado y utilizado para justificar una vigilancia masiva que atente contra los derechos fundamentales de la privacidad y el libre tránsito, especialmente en el Norte Global, y que esto afecte desproporcionadamente a poblaciones migrantes y desplazadas. Es crucial que se establezcan salvaguardas claras y estrictas para prevenir la instrumentalización de estas medidas contra grupos vulnerables, asegurando que cualquier acción tomada en el marco de esta convención se realice con pleno respeto a los derechos humanos y las libertades fundamentales, conforme a los principios establecidos en la Carta de las Naciones Unidas.

El cibercrimen es un fenómeno que puede afectar las actividades cotidianas, comprometer la privacidad y violar los derechos de quienes usan las tecnologías e internet. Dados sus alcances (que oscilan entre el fraude con fines económicos, pasando por el ciberacoso y hasta los delitos más graves relacionados con la explotación sexual de menores y otros que ponen en riesgo y vulneran profundamente los derechos y la dignidad de las personas), es de esencial importancia que la Convención Internacional Comprensiva Sobre La Lucha Contra El Uso De Las Tecnologías De La Información Y Las Comunicaciones Con Fines Delictivos haga referencia explícita a los marcos internacionales de derechos humanos, por ejemplo, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) de las Naciones Unidas. Esto, con objetivos de que las medidas contra el cibercrimen se alineen con los estándares internacionales de derechos humanos, se refuerce la legitimidad de estas y se fomente la cooperación entre los Estados Parte.

DOI: 10.5281/zenodo.12668116

En segundo lugar, es necesaria la actualización continua de las definiciones y medidas contra el cibercrimen, ya que en el ciberespacio las dinámicas de convivencia, socialización, transacción e incluso toma de decisiones y desarrollo de actividades del ámbito social, político y cultural, se renuevan y transforman con velocidad, lo cual ha generado brechas y desigualdades en términos de acceso e impartición de justicia cuando los derechos fundamentales son vulnerados. Esto implica también la clarificación de términos clave, empezando por cibercrimen y sus modalidades para evitar un uso ambiguo que dé pie a interpretaciones equívocas. Para ello, se propone la utilización de ejemplos cuando se empleen términos técnicos.

Se sugiere con especial hincapié clarificar el alcance de la definición de delitos, especificando que estos pueden ser cometidos por personas naturales, jurídicas, entidades estatales y paraestatales. Además, incluir el espionaje perpetrado por estas entidades contra activistas, periodistas y otros actores de la sociedad civil.

Es crucial que se incluya la implementación de programas educativos y de concientización sobre la seguridad en las TIC y la prevención del cibercrimen. Estos programas deben estar diseñados para informar a los usuarios sobre los riesgos asociados al uso de las TIC, e incluir recomendaciones y medidas preventivas en los diferentes ámbitos de desarrollo de los usuarios. Pero también es esencial contar con procedimientos para poder recuperar y conservar la información, según sea el caso, para minimizar el impacto de cualquier incidente en el ciberespacio o híbrido.

En este sentido, otro de los aspectos de relevancia es el apoyo integral a las víctimas de cibercrímenes, incluyendo servicios de asesoramiento y asistencia legal. Para que esto sea efectivo, se considera que los programas de prevención deben de estar respaldados con la capacitación en derechos humanos de las fuerzas del orden, jueces, fiscales y personal de atención a las víctimas, como médicos, psicólogos y trabajadores sociales, de manera continua sobre los derechos y necesidades de las víctimas, para fomentar una cultura de empatía y apoyo, con el objetivo de promover una cultura de respeto y protección en todas las acciones y decisiones relacionadas.

El derecho al acceso a la justicia está contemplado dentro del Pacto Internacional de Derechos Civiles y Políticos y de la Declaración Universal de Derechos del Hombre, y por ende, los Estados Parte deben garantizar que las personas (sin distinción por nacionalidad, origen étnico, origen migratorio, género, credo o ideología) puedan acceder y defender sus derechos en procesos justos e imparciales.

Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Germany | contact@knowmadinstitut.org | knowmadinstitut.org
DOI: 10.5281/zenodo.12668116

Esto se relaciona con las sanciones derivadas de dichos procesos, las cuales deben ser proporcionales y efectivas, ya que no todos los cibercrímenes tienen el mismo impacto y por ello, las sanciones pueden oscilar entre medidas complementarias vinculadas con programas de educación sobre ciberseguridad, penas económicas disuasivas para restitución a las víctimas del cibercrimen e incluso penas de prisión.

Hacemos un llamado a los Estados Parte para que, al formular y aplicar las medidas contra el cibercrimen, mantengan un enfoque centrado en los derechos humanos, protegiendo y promoviendo la dignidad de cada individuo. Solo así podremos construir un entorno digital seguro y justo para todos.

European Institute for Multidisciplinary Studies on Human Rights and Sciences - Knowmad Institut.

Grupo Especial de Trabajo:
Ob. Martin Ignacio Díaz Velásquez, Prof. Jorge Vicente Paladines, Dra. Leticia Fuentes Vera, Ing. Jesús Alfredo Ribero Faria, MSc. Oscar Hugo Espin García, Rev. Daniela Kreher, MSc. Ludwing Moncada Bellorin.

Nota: Este documento es una versión resumida de nuestro análisis y comentarios detallados que se pueden encontrar aquí.

REFERENCIAS

1. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., & Rifat, N. (2022). Cybersecurity threats and their mitigation approaches using machine learning—A review. *Journal of Cybersecurity and Privacy, 2*(3), 527-555. https://doi.org/10.3390/jcp2030027
2. Ali, A., Khan, I., & Bashir, S. (2022). Need of international legislation regarding cyber crimes: Pakistan perspective. *Pakistan Journal of Social Research, 4*(2), 45-55. https://doi.org/10.52567/pjsr.v4i2.608
3. Aldridge, J., Stevens, A., & Barratt, M. J. (2017). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction, 113*(5), 789-796. https://doi.org/10.1111/add.13899

DOI: 10.5281/zenodo.12668116

4. Ajoy, P. B. (2022). Effectiveness of criminal law in tackling cybercrime: A critical analysis. *Scholars International Journal of Law, Crime and Justice, 5*(2), 75-85. https://doi.org/10.36348/sijlcj.2022.v05i02.005
5. Aulia, A. (2023). Adoption of the law on information and electronic transactions against cyber crime. *Scholars International Journal of Law, Crime and Justice, 6*(3), 1-7. https://doi.org/10.36348/sijlcj.2023.v06i03.001
6. Balajanov, E. (2018). Setting the minimum age of criminal responsibility for cybercrime. *International Review of Law, Computers & Technology, 32*(1), 102-115. https://doi.org/10.1080/13600869.2018.1417764
7. Brenner, S. W., & Clarke, L. L. (2009). Combatting cybercrime through distributed security. *International Journal of Intercultural Information Management, 1*(3), 259. https://core.ac.uk/download/pdf/76622895.pdf
8. Broadhurst, R. (2017). Cybercrime: Thieves, swindlers, bandits and privateers in cyberspace. *SSRN*. https://doi.org/10.2139/ssrn.3009574
9. Bunga, D. (2019). Legal response to cybercrime in global and national dimensions. *Padjadjaran Journal of International Law, 6*(1), 45-57. https://doi.org/10.22304/pjih.v6n1.a4
10. Bunga, D., & Hiariej, O. S. (2019). Cyberbullying on children in victimology perspective. *Scholars International Journal of Law, Crime and Justice, 2*(2), 116-121. https://doaj.org/article/74dfa3150c9d4afdabdb5a24672dae82
11. Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice, 13*(1), 66-79. https://doi.org/10.1093/police/pax055
12. Cerezo, A., Lopez, J., & Patel, A. (2007). International cooperation to fight transnational cybercrime. *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.1109/WDFIA.2007.7
13. Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review, 49*, 345+. U of Maryland Legal Studies Research Paper No. 2014-1. https://ssrn.com/abstract=2368946
14. Clough, J. (2015). Principles of cybercrime: Interception of data. *Cambridge University Press*. https://doi.org/10.1017/CBO9781139540803.007
15. Cross, D. (2017). A human rights-based approach to community justice: Adding value to desistance focused practice. *European Journal of Probation, 9*(2), 67-84. https://doi.org/10.1177/2066220317719801
16. Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573-592. https://doi.org/10.1177/0032258X221107584
17. Da-Yu Kao, E., Chang, E.-C., & Tsai, F. (2019). Extracting suspicious IP addresses from WhatsApp network traffic in cybercrime investigations. *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/ICACT.2019.8701941

DOI: 10.5281/zenodo.12668116

18. Dragomir, B. (2022). Mechanisms of international cooperation against cybercrime. *Proceedings of the International Conference on Cybercrime, 70*(1), 55-68. https://doi.org/10.36997/ppdd2022.70
19. ECPAT International. (2016). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales. *ECPAT Luxembourg*. https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines_Spanish_version-electronica_FINAL.pdf
20. Feldle, J. (2020). Zivilrechtliche Haftung im automatisierten Straßenverkehr – Hackerangriffe, Sicherheitserwartungen und erlaubte Nebentätigkeiten. *Nomos*. https://doi.org/10.5771/9783748920984-199
21. Geldenhuys, K. (2021). Spyware. *Servamus Community-Based Safety and Security Magazine, 114*(10), 15-17. https://doi.org/10.10520/ejc-servamus_v114_n10_a5
22. Grauer, K. (2022). The 2022 crypto crime report. *Chainalysis*. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf
23. Gunarto, G., Jainah, J., & Mashdurohatun, A. (2023). Legal reconstruction of trafficking victim protection based on justice value. *Scholars International Journal of Law, Crime and Justice, 6*(5), 25-32. https://doi.org/10.36348/sijlcj.2023.v06i05.005
24. Han, Y. (2023). Research and application of pseudo-information detection technology based on computer information hiding. *Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.1109/ACCTCS58815.2023.00067
25. Henry, N., Flynn, A., & Powell, A. (2020). Technology-facilitated domestic and sexual violence: A review. *Violence Against Women, 26*(7), 761-788. https://doi.org/10.1177/1077801219841445
26. Holt, T. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *Annals of the American Academy of Political and Social Science, 678*(1), 140-157. https://doi.org/10.1177/0002716218783679
27. Hursevich, A. (2019). Ube international legal cooperation of the prosecutor general's office of the republic of belarus in the fight against cybercrime and typical examples of committing such crimes. *RAESMPCE, 11*(2). https://doi.org/10.54275/raesmpce.v11i2.96
28. Irawan, J., Nathaniel, A., & Jonathan, S. (2022). Juridical analysis about cyberbullying cases by child perpetrators against child victims. *De Jure: Jurnal Hukum Dan Siyasah, 22*(1), 17-32. https://doi.org/10.30641/dejure.2022.v22.17-32
29. Interpol. (2022). Terminología apropiada. Recuperado de https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada
30. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2020). A review on cyber crimes on the internet of things. *ArXiv*. https://arxiv.org/abs/2009.05708
31. Kaur, S. (2021). Security in cyber crime. *International Journal of Recent Advances in Science and Technology, 9*(5), 123-135. https://doi.org/10.22214/ijraset.2021.38023
32. Kennedy, S., & Warren, I. (2020). The legal geographies of extradition and sovereign power. *Internet Policy Review, 9*(3), 1-22. https://doi.org/10.14763/2020.3.1496

DOI: 10.5281/zenodo.12668116
33. Khan, S., Saleh, T., Dorasamy, M., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000Research, 11*, 971. https://doi.org/10.12688/f1000research.123098.1
34. Klevtsov, K. (2020). International cooperation in the fight against cybercrime: Current state and development prospects. *SSRN*. https://doi.org/10.2139/ssrn.3728311
35. Knowmad Institut. (2023). TERCERA SESIÓN: COOPERACIÓN INTERNACIONAL, ASISTENCIA TÉCNICA, MEDIDAS DE PREVENCIÓN Y MECANISMO DE APLICACIÓN. Recuperado de https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/Knowmad-_ES_3rd_Session.pdf
36. Krastev, D. B. (2022). Mechanisms of international cooperation against cybercrime. *International Journal of Cybersecurity, 70*(2), 155-167. https://doi.org/10.36997/ppdd2022.70
37. Lobach, D. V., Shestopal, S. S., & Smirnova, N. L. (2021). The phenomenon of cyber crime in the focus of conceptual legal analysis. *European Proceedings of Social and Behavioural Sciences, 6*(3), 385-392. https://doi.org/10.15405/epsbs.2021.06.03.77
38. Mabeka, N. Q., & Cassim, F. (2023). Interpreting the provisions of the Cybercrimes Act 19 of 2020 in the context of civil procedure: A future journey. *Obiter, 44*(1). https://doi.org/10.17159/obiter.v44i1.15886
39. Mantovani, M. (2020). Contractual obligations as a tool for international transfers of personal data under the GDPR. *SSRN*. https://doi.org/10.2139/ssrn.3522426
40. McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies, 37*(3), 534-561. https://doi.org/10.1093/ojls/gqw033
41. Meier, B. M., Huffstetler, H. E., & de Mesquita, J. B. (2020). Monitoring and review to assess human rights implementation. *International Journal of Human Rights, 24*(3), 256-270. https://doi.org/10.1093/oso/9780197528297.003.0008
42. Montal, F., & Pauselli, G. (2023). Is the bad news about compliance bad news about human rights? Evidence from the Inter-American Commission on Human Rights. *International Studies Quarterly, 67*(1), 85-97. https://doi.org/10.1093/isq/sqad027
43. Naciones Unidas. (1966). Pacto Internacional de Derechos Civiles y Políticos. Recuperado de https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
44. Naciones Unidas. (1966). Pacto Internacional de Derechos Civiles y Políticos. Recuperado de https://www.ohchr.org/sites/default/files/ccpr_sp.pdf
45. Naciones Unidas. (2016). Promoción, protección y disfrute de los derechos humanos en Internet. *A/HRC/32/L.20*. Recuperado de https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf
46. Nurahman, D. (2019). Kebijakan penegakan hukum cybercrime dan pembuktian yuridis dalam sistem hukum pidana nasional. *Jurnal Keadilan, 17*(2), 270-284. https://doi.org/10.37090/keadilan.v17i2.270
47. Nurahman, D. (2020). Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. *CCER*, 101. http://dx.doi.org/10.4108/eai.26-9-2020.2302579

DOI: 10.5281/zenodo.12668116

48. PTACC | Police Treatment and Community Collaborative. (2022). Best practices in law enforcement and community responses. Recuperado de https://ptaccollaborative.org/
49. Ruslan, A. R. (2023). International legal regulation of the fight against cybercrime. *Journal of International Law, 24*(3), 24-30. https://doi.org/10.37399/issn2072-909x.2023.4.24-30
50. Sabu, J., Ananthanarayanan, S., Gopan, A., G. S., & Murali, S. (2023). Advanced keylogger with keystroke dynamics. *Proceedings of the International Conference on Information and Communication Technology*. https://doi.org/10.1109/ICICT57646.2023.10134044
51. Sarkar, G., & Shukla, S. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*, 1-26. https://doi.org/10.1016/j.jeconc.2023.100034
52. Saxena, M. (2023). Impact of cybercrime on e-governance. Is cybercrime affecting the confidentiality of government data? *International Journal of Cyber Criminology*. https://doi.org/10.21275/sr231111140516
53. Setiawahyudi, A. (2015). Kendala pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet berdasarkan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Majalah Hukum, 21*(2), 145-167. https://dx.doi.org/10.30996/mk.v0i0.2116
54. Skulysh, I. (2014). International legal cooperation in the field of combating cybercrime. *Journal of Law and Political Sciences, 10*(1), 272-432. https://doi.org/10.37750/2616-6798.2014.1(10).272432
55. Snail, S. (2009). Cyber crime in South Africa - Hacking, cracking, and other unlawful online activities. *Journal of Information Law & Technology, 10*(2), 127-145. https://dblp.org/rec/journals/jilt/Snail09.html
56. Sprott, J. B. (2006). The use of custody for failing to comply with a disposition cases under the Young Offenders Act. *Canadian Journal of Criminology and Criminal Justice, 48*(3), 251-271. https://doi.org/10.1353/ccj.2006.0043
57. Szongoth, R., & Vetter, D. (2018). Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. *Budapesti Szemle, 7-8*(1), 45-60. https://doi.org/10.38146/bsz.2018.7-8.1
58. Teichmann, F., & Wittmann, C. (2022). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime, 29*(3), 819-832. https://doi.org/10.1108/jfc-04-2022-0093
59. Tiutiuhin, V. I. (2022). Conviction as one of the means of criminal responsibility. *Journal of Law and Political Sciences, 18*(1), 267-249. https://doi.org/10.21564/2311-9640.2022.18.267249
60. UNODC. (2021). World drug report 2021. *United Nations: Office on Drugs and Crime*. https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html
61. Varshney, S., Munjal, D., Jash, I., Bhattacharya, O., & Saboo, S. (2020). Cyber crime awareness and corresponding countermeasures. *SSRN*. https://doi.org/10.2139/ssrn.3601807
62. Veresha, R. (2018). Preventive measures against computer related crimes. *Interdisciplinary Management Research, 14*, 227-243. https://doi.org/10.32914/I.51.3-4.7

DOI: 10.5281/zenodo.12668116

63. Voynova, R. (2015). Comparison of the transfer of criminal proceeding with other forms of international legal cooperation in criminal matters. *Sciendo*. https://doi.org/10.1515/kbo-2015-0091
64. Weber, R. (2009). Internet of things–Need for a new legal environment? *Computer Law & Security Review, 25*(6), 522-527. https://doi.org/10.1016/j.clsr.2009.09.002
65. Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?. *Int. Cybersecur. Law Rev.* 1, 63–72. https://doi.org/10.1365/s43439-020-00012-5
66. Wilson, N. (2008). Forensics in cyber-space: The legal challenges. *International Journal of Digital Crime and Forensics, 3*(1), 56-70. https://doi.org/10.4108/E-FORENSICS.2008.2926
67. Wingfield, T., & Wingo, H. (2021). International law for cyberspace. *Oxford Handbook of Cybersecurity*. https://doi.org/10.1093/oxfordhb/9780198800682.013.37