Contribución conjunta de Derechos Digitales, R3D, IPANDETEC e Hiperderecho para el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos - Sexto período de sesiones

Introducción

Las organizaciones **Derechos Digitales**, **Red en Defensa de los Derechos Digitales (R3D)**, **Instituto Panamericano de Derecho y Tecnologías (IPANDETEC) e Hiperderecho**, pertenecientes a AlSur[1], un consorcio de 11 organizaciones de la sociedad civil y del ámbito académico que desde América Latina buscan fortalecer los derechos humanos en el entorno digital de la región, agradecen la oportunidad de presentar sus propuestas con miras a la sexta reunión del Comité Especial encargado de elaborar una convención internacional general sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos.

En relación al Proyecto de texto de la convención, documento A/AC.291/22, las organizaciones firmantes desean formular las siguientes recomendaciones sustanciales para someterlas a la consideración de los Estados Miembros:

a) **Incorporar** la perspectiva de género en toda la convención en su conjunto y a través de cada artículo en los esfuerzos para prevenir y combatir la ciberdelincuencia.

Agregar "perspectiva de género" en los artículos **24 y 36.**

Incluir una disposición específica que haga hincapié en que los derechos de las mujeres y las niñas son derechos humanos y que las mujeres y las niñas corren un mayor riesgo de sufrir violencia facilitada por la tecnología, especialmente las adolescentes y las mujeres y las niñas que se enfrentan a formas diferentes e interrelacionadas de discriminación en el **artículo 5.**

Incluir disposiciones que especifiquen que los Estados tienen la posibilidad de denegar la solicitud de asistencia judicial si existen serias dudas de que la solicitud pueda basarse en una discriminación por razón de sexo u orientación sexual en **el artículo 40.**

Reincorporar la necesidad de incorporar métodos para integrar la perspectiva de género en la elaboración de políticas, la legislación y la programación en el **artículo 54.**

b) En el **Capítulo II sobre criminalización**, recomendamos **realizar cambios** en los **Artículos 6, 8 y 9** con respecto al término "intención deshonesta" y sustituirlo por "intención dolosa" para reducir el margen de interpretación; **evaluar la permanencia de los Artículos 10 al 16** debido a que estos repiten delitos ya mencionados y porque contienen conductas criminales comunes; **establecer una excepción** para los casos de difusión de material en el **Artículo 15** pues estos abren la puerta a revictimización y criminalizan a las propias víctimas; **eliminar el Artículo 17**, así

[1] Ver: https://www.alsur.lat/.

como **los incisos b y c del Artículo 23**, pues estos atentan contra la garantía del ejercicio de la libertad de expresión.

c) **En el capítulo IV de Medidas Procesales y aplicación de la ley recomendamos: Artículo 23:** es necesario eliminar los incisos b y c a fin de garantizar que las medidas procedimentales solo sean aplicadas a los delitos cubiertos por la Convención. **Artículo 24: es necesario agregar en el primer párrafo que las condiciones y salvaguardas acorde** al derecho internacional y la perspectiva de género deban ser incluidas en legislaciones locales. Así mismo recomendamos que se reincorporen las referencias a los principios de legalidad, proporcionalidad y necesidad. En el segundo párrafo, aclarar que las condiciones y salvaguardias expresadas en este artículo se aplican a todos los procedimientos o facultades previstos en el Convenio y son necesarias para una debida justificación del uso de las medidas procedimentales. **Artículo 29:** agregar que el artículo será aplicado a los delitos contenidos en los artículos 6 a 16. **Artículo 30:** sustituir "en relación a delitos graves que determinará en su derecho interno" por "en relación a los artículos 6 y 16 de esta Convención"

d) En relación a la **Cooperación internacional**, recomendamos eliminar la referencia al artículo 17 en el **Artículo 35** y agregar el requisito de doble criminalidad para poder llevar adelante la cooperación internacional. **Además recomendamos incluir en el Artículo 36** la mención expresa al derecho internacional de los derechos humanos bajo una perspectiva de género. Asimismo, el principio de protección de datos personales es internacional y debe ser reconocido en el texto expresamente.

1. **Perspectiva de género (*gender mainstream*)**

Recomendaciones:

- Incorporar la perspectiva de género en toda la convención en su conjunto y a través de cada artículo en los esfuerzos para prevenir y combatir la ciberdelincuencia.
- Incluir una disposición específica que haga hincapié en que los derechos de las mujeres y las niñas son derechos humanos y que las mujeres y las niñas corren un mayor riesgo de sufrir violencia facilitada por la tecnología, especialmente las adolescentes y las mujeres y las niñas que se enfrentan a formas diferentes e interrelacionadas de discriminación en el **artículo 5.**
- Incluir la referencia a "necesidad de aplicar la perspectiva de género" en los **artículos 24 y 36.**
- Incluir disposiciones que especifiquen que los Estados tienen la posibilidad de denegar la solicitud de asistencia judicial si existen serias dudas de que la solicitud pueda basarse en una discriminación por razón de sexo u orientación sexual en **el artículo 40.**
- Reincorporar la necesidad de incorporar métodos para integrar la perspectiva de género en la elaboración de políticas, la legislación y la programación en el **artículo 54.**

Rationale:

Si bien celebramos la inclusión de la importancia de incorporar una perspectiva de género en el preámbulo del borrador cero, esta sola referencia es insuficiente para asegurar que la

Convención no sea utilizada en detrimento de los derechos humanos de las personas en base al género.

Es esencial incorporar la perspectiva de género[2] en toda la convención en su conjunto y a través de cada artículo. Esto permitirá que la Convención aborde las necesidades y prioridades específicas de las mujeres y de las personas pertenecientes a la comunidad LGBTQIA+ así como los impactos diferenciados del cibercrimen en función del género en conjunción con otras interseccionalidades. Esto conducirá a una aplicación más efectiva de la Convención, así como a proporcionar garantías especiales de protección a los grupos en situación de vulnerabilidad.

Tanto los espacios digitales como los sistemas penales se insertan en sociedades que dan cuenta de desigualdades estructurales preexistentes. Ni las tecnologías digitales ni las leyes y normas que las rigen son neutrales: tienen el potencial de promover el ejercicio de los derechos humanos, pero también pueden perpetuar y agravar las desigualdades estructurales. Teniendo esto en cuenta, **Derechos Digitales y APC** han enfatizado anteriormente[3] que **un elemento central de esta futura convención debería ser la integración de una perspectiva de género, cuyo objetivo es avanzar hacia la igualdad de género.**

La incorporación de la perspectiva de género permitirá que la Convención aborde las realidades, necesidades y prioridades específicas de las mujeres y de las personas pertenecientes a la comunidad LGBTQIA+, así como los impactos diferenciados en función del género en conjunción con otras interseccionalidades. En este sentido, la Convención debe procurar generar una base legal que obligue a los países firmantes a regular sus procesos de denuncia, investigación, sanción y cumplimiento de sentencia con perspectiva de género. Esto conducirá a una aplicación más efectiva de la Convención, así como a proporcionar garantías especiales de protección a los grupos en situación de vulnerabilidad.

Para ello planteamos que la referencia a la necesidad de aplicar la perspectiva de género sea agregada a artículos que consideramos que necesitan garantías especiales de protección por sus capacidades de profundizar desigualdades de género. Esto, con el fin de evitar que en la aplicación de la Convención se vulneren otros derechos humanos.

2. **Criminalización.**

Recomendaciones:

- **Artículos 6, 8 y 9:** eliminar la expresión “intención deshonesta” y sustituirla por “intención dolosa”.
- **Artículo 10:** evaluar si es necesaria su permanencia en la Convención dado que los delitos que busca combatir ya están consagrados en los artículos 6 al 9 de la misma y su permanencia criminaliza la tecnología.

---

[2] La transversalidad de género se entiende como una estrategia para hacer de las preocupaciones y experiencias de mujeres y hombres una dimensión integral del diseño, la implementación, el seguimiento y la evaluación de políticas y programas en todas las esferas políticas, económicas y sociales, de modo que no se perpetúe la desigualdad. Ver: https://www.un.org/womenwatch/daw/csw/GMS.PDF

[3] Contribución conjunta de Derechos Digitales y la Asociación para el Progreso de las Comunicaciones (APC). Quinta sesión del Comité Especial AHC. Disponible en: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main

- **Artículo 15:** eliminar la referencia de la intención de causar daño y establecer una excepción para los casos de difusión de material mediante denuncias realizadas por las víctimas o periodistas.
- **Artículos del 11 al 16:** es necesario que los Estados evalúen la permanencia de los mismos en el Convenio, porque contienen conductas criminales comunes que pueden ser cometidas a través de las tecnologías.
- **Artículo 17:** es necesario que se elimine el artículo en su totalidad.
  Rationale:

En el capítulo de **Criminalización (Art 6-21**) celebramos la reducción del catálogo de delitos en la nueva versión de la presidencia de 30 a 11 delitos.

El nuevo texto se centra en lo general en delitos cometidos a través y contra sistemas informáticos (ciberdelitos)[4]. Celebramos que el texto actual evite incluir delitos relacionados con el contenido que criminalicen actividades relacionadas con el ejercicio legítimo de derechos de la ciudadanía.

Sin embargo, en algunos de los delitos incluidos en el primer borrador persisten ambigüedades en la redacción que podrían criminalizar la labor de periodistas e investigadores de seguridad digital, así como defensores de derechos humanos, activistas y periodistas. Con la consecuente generación de impactos diferenciados de género y revictimizaciones.

Latinoamérica se ha ido consolidando como una región peligrosa para el ejercicio de defensa de derechos por parte de activistas, periodistas, defensores e investigadores. Esto debido a que, desde los Gobiernos, se han llevado a cabo diversos mecanismos de represión y obstaculización frente al ejercicio de los derechos civiles de los ciudadanos. La criminalización y la vigilancia constituyen mecanismos para obstaculizar la labor que realizan estos actores en defensa de la democracia y el Estado de Derecho.

Actualmente, hacen falta instrumentos penales con enfoque diferencial de género y de derechos humanos. La tendencia legislativa actual permite el aumento de uso arbitrario por parte de los Estados de tecnologías de vigilancia en vez de evitar la persecución judicial de actores con posturas y opiniones críticas a los Estados.

Organizaciones de toda la región[5] latinoamericana han denunciado a la CIDH repetidamente casos graves de estos usos arbitrarios: persecuciones judiciales a periodistas, el uso de leyes de contenido contra activistas mujeres y LGBTQIA+ para criminalizar expresiones

[4] Human Rights Watch. Letter to the UN Ad Hoc Commitee on Cibercrime. Disponible en: https://www.hrw.org/news/2022/01/13/letter-un-ad-hoc-committee-cybercrime

[5] **D**enunciaron ante la CIDH el avance del "acoso judicial" contra periodistas en América Latin. Clarín. Disponible en: https://www.clarin.com/politica/denunciaron-cidh-avance-acoso-judicial-periodistas-america-latina_0_en4HJXFUSv.html. Article 19. Acoso judicial a periodistas y defensores(as) de derechos humanos, la víctima es la libertad de expresión. Disponible en: https://articulo19.org/acoso-judicial-a-periodistas-y-defensoresas-de-derechos-humanos-la-victima-es-la-libertad-de-expresion/

legítimas a nivel regional y global[6], la persecusión a denunciantes o <<whistleblowers>>[7], el uso de software Osint para investigaciones[8]-[9], el uso de spyware[10] o la judicialización de investigadores[11].

La criminalización generada por el abuso de estas legislaciones ya ha sido identificada por mecanismos de DDHH como una "tendencia creciente en todo el mundo", que ha abierto la puerta a vigilar y castigar a los activistas, provocando un importante efecto amedrentador sobre la defensa y la movilización, obstaculizando el trabajo de los defensores de los derechos humanos y poniendo en peligro su seguridad de manera contraria al derecho internacional[12].

Una reciente investigación[13] de Derechos Digitales y APC visibiliza la necesidad de considerar los impactos de género de esta criminalización, sobre la base de que la libertad de expresión es esencial para la igualdad de género. El informe aporta pruebas concretas, a través de 11 casos mapeados a nivel global, de la tendencia del uso de estas normativas como herramienta legal para silenciar voces críticas, lo que afecta de manera diferencial al activismo de grupos históricamente excluidos del debate público como las mujeres y las personas LGBTQIA+. Los casos demuestran que no estamos hablando de riesgos potenciales, sino de efectos concretos, lo que da la voz de alarma sobre los peligros inherentes a avanzar en las normas internacionales sobre la materia sin tener en cuenta los contextos nacionales ni incluir salvaguardias para la protección de los derechos humanos, en particular de los grupos históricamente marginados.

La garantía del ejercicio de la libertad de expresión requiere necesariamente de un entorno seguro y propicio para ser efectiva. Por ello, las legislaciones que criminalizan la capacidad de expresar demandas sociales relacionadas con desigualdades estructurales -ya sea por el contenido de la expresión o por el género de la persona que expresa su opinión- excluyen a las mujeres, ya que las restricciones ilegítimas atentan directamente contra su visibilidad y plena participación en la vida pública[14]. Siguiendo a la Corte Interamericana de Derechos

---

[6] Derechos Digitales. Normativas contra los ciberdelitos como herramientas para silenciar mujeres y personas LGBTQIA+ alrededor del mundo, 5 de Julio 2023. Disponible en: https://www.derechosdigitales.org/21876/cuando-la-proteccion-se-transforma-en-amenaza-normativas-contra-los-ciberdelitos-como-herramientas-para-silenciar-mujeres-y-personas-lgbtqia-alrededor-del-mundo/

[7] CIDH. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/180.asp

[8] https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/

[9] https://datysoc.org/informe-ciberpatrullaje/

[10] https://www.nytimes.com/es/2023/04/18/espanol/pegasus-mexico-gobierno-ejercito.html

[11] https://www.youtube.com/watch?v=mVNzL0l5U3k

[12] ONU - Asamblea General. Aplicación de la Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, proporcionando un entorno seguro y propicio a los defensores de los derechos humanos y garantizando su protección. A/RES/74/146. Disponible en: https://digitallibrary.un.org/record/3847133

[13] Derechos Digitales. Normativas contra los ciberdelitos como herramientas para silenciar mujeres y personas LGBTQIA+ alrededor del mundo, 5 de Julio 2023. Disponible en: https://www.derechosdigitales.org/21876/cuando-la-proteccion-se-transforma-en-amenaza-normativas-contra-los-ciberdelitos-como-herramientas-para-silenciar-mujeres-y-personas-lgbtqia-alrededor-del-mundo/

[14] CIDH. Relatoría Especial para la Libertad de Expresión. Relatoría Especial para la Libertad de Expresión expresa preocupación por investigación penal iniciada en Chile contra miembros de Las Tesis. Comunicado de prensa R152/20. Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?lID=2&artID=1178

Humanos, una de las principales consecuencias del silenciamiento es que “conduce a un aumento de la brecha de género (...) y atenta contra el pluralismo como elemento esencial de la libertad de expresión y la democracia"[15].

El borrador cero incluye un nuevo artículo sobre **Delitos relativos a otros tratados internacionales (Art. 17)** con el cual se abre una brecha para aplicar la Convención a otras conductas no contempladas en la misma, generando riesgos de criminalización.

El **artículo 17** establece la obligación de los Estados de tomar las medidas necesarias para tipificar y perseguir las conductas calificadas como delitos en “tratados y protocolos internacionales” cuando se cometan mediante el uso de tecnologías. Esta redacción es ambigua y supone un grave riesgo a la soberanía de los países y a los derechos humanos.

La amplitud de la redacción habilita a que puedan incorporarse todos aquellos delitos de contenido que se encontraban en la lista en versiones anteriores además de cualquier otro delito que se reconozca en otro tratado, incluso sin que los Estados Parte de la Convención lo hayan acordado.

Por ejemplo, teniendo en cuenta que existen convenios relativos a asuntos como terrorismo o la trata de personas, entre muchos otros, algunas de las conductas excluidas directamente del texto del convenio de ciberdelitos podrían terminar siendo reincorporadas a nivel nacional[16]. A su vez, el artículo no contiene una limitación de tiempo por lo que futuros tratados, creados por ejemplo de manera bilateral, podrían ser incluidos.

Por tanto, se debe garantizar que el contenido de la Convención permita avanzar en la defensa de derechos humanos y no en la legitimación del aumento de mecanismos de criminalización del ejercicio de los derechos. Para lograrlo es necesario incluir no sólo la perspectiva de derechos humanos y de género de manera interseccional, sino que es urgente tomar en cuenta el contexto histórico y político de los distintos países de América Latína.

En consecuencia, a continuación presentamos nuestras recomendaciones desglosadas al *Capítulo II Criminalización.* Las propuestas de redacción a este capítulo se pueden encontrar en el **ANEXO I** al final del documento.

Artículos 6, 8 y 9

Los delitos de **Acceso ilícito (Art. 6)**, **Interferencia con datos o información (Art. 8)**, **Interferencia con un sistema o dispositivo (Art. 9)** están la fórmula de <<deliberado y sin derecho>> (*Intentionally and without right*) y con <<intención deshonesta>> (*dishonest*

[15] Corte Interamericana de Derechos Humanos. Caso Bedoya Lima y otros vs. Colombia. Sentencia de 26 de agosto de 2021, par. 113. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_431_ing.pdf

[16] Un ejemplo del posible uso abusivo de la legislación referente a terrorismo asociada a internet es el caso de las judicializaciones durante las protestas en Colombia en 2021. Al respecto, expertos de la ONU han expresado públicamente su preocupación respecto al uso de disposiciones antiterroristas para procesar manifestantes. Disponible en: https://www.ohchr.org/es/press-releases/2023/03/colombia-misuse-counter-terrorism-measures-prosecute-protesters-threatens

intent) deja la puerta abierta para interpretaciones arbitrarias que dificulten las labores de investigación[17].

Teniendo en cuenta que las personas defensoras, investigadores, activistas y periodistas pueden ser criminalizadas mediante estos delitos, es necesario que “Intención deshonesta” sea sustituida por “intención dolosa o maliciosa”. Además, la redacción debe incluir disposiciones específicas que explícitamente protejan las actividades legítimas de investigación por parte de la ciudadanía.

De igual forma, debe de incorporar el elemento de daño material para evitar la criminalización de las actividades de investigadores de seguridad.

Artículo 10 (delito de uso indebido de dispositivos)

Este artículo contiene redacción ambigua y amplia que podría criminalizar la adquisición y uso de tecnologías que permitan el ejercicio o protección de derechos humanos. Principalmente, se pone en riesgo a actores esenciales para un internet libre y seguro como lo son las personas investigadores de seguridad, periodistas o personal académico.

Es necesario que no se criminalice la herramienta y se entienda el alcance que pueden tener estos desarrollos tecnológicos para una sociedad democrática. El uso de palabras como <<posesión>>, <<obtención>>, <<producción>>, <<venta>>, <<adquisición>>. criminalizan la herramienta y no su uso con intenciones maliciosas y que resuelven en un daño material.

Artículo 15 (difusión no consentida de imágenes de carácter íntimo)

Reconocemos que el delito de **Difusión no consentida de imágenes de carácter íntimo (Art. 15)** es sumamente grave para la región. Por lo cual, el texto debe ser refinado para la correcta y exacta aplicación a esta conducta evitando que resulte en revictimización o criminalizando actividades legítimas de las víctimas y sus acompañantes.

En primer lugar, el término desnudez tiende a tener una interpretación ambigüa. Este concepto puede excluir contenido sexual de personas que no estaban desnudas completamente o incluir contenido no sexual, ni íntimo de partes como brazos, piernas, hombros que no estén cubiertos por ropa. Si bien es vital mantener el elemento del consentimiento de la víctima, también hay que especificar las conductas que serán perseguidas.

Igualmente, el delito no establece excepciones legítimas a los casos de difusión que pueden resultar en la criminalización de las mismas víctimas, sus acompañantes o periodistas. Por ejemplo, el compartir evidencia a sus asesores legales donde se encuentre contenido de otras personas además del de la víctima.

Finalmente, es vital que el texto elimine la intencionalidad de causar un daño como requisito necesario para este delito y lo sustituya por “a sabiendas de la falta de consentimiento de la víctima”. La afectación a la persona víctima de este delito ocurre desde el momento en el que se comparte el contenido sin su consentimiento. Muchos de estos casos suceden en secreto a espaldas de la víctima con fines distintos a causarle un daño directo. Por lo tanto,

[17] Para más información sobre los riesgos legales para investigadores de ciberseguridad recomendamos consultar la siguiente fuente: https://github.com/disclose/research-threats

añadirle un requisito de intencionalidad impone a las víctimas una carga probatoria injustificada.

Delitos relativos a otros tratados internacionales (Art. 17)

Recomendamos enfáticamente eliminar este artículo. Esta disposición abre la puerta a la inclusión de delitos que no son ciberdependientes, pueden ser aplicados de manera arbitraria y atenten contra la soberanía y derechos humanos en los Estados Parte.

3. **Medidas Procesales y aplicación de la ley (Capítulo IV)**

Recomendaciones:

- **Artículo 23:** es necesario eliminar los incisos b y c a fin de garantizar que las medidas procedimentales solo sean aplicadas a los delitos cubiertos por la Convención.
- **Artículo 24: es necesario agregar en el primer párrafo que las condiciones y salvaguardas acorde** al derecho internacional y la perspectiva de género deban ser incluidas en legislaciones locales. Así mismo recomendamos que se reincorporen las referencias a los principios de legalidad, proporcionalidad y necesidad. En el segundo párrafo, aclarar que las condiciones y salvaguardias expresadas en este artículo se aplican a todos los procedimientos o facultades previstos en el Convenio y son necesarias para una debida justificación del uso de las medidas procedimentales.
- **Artículo 29:** agregar que el artículo será aplicado a los delitos contenidos en los artículos 6 a 16.
- **Artículo 30:** sustituir “en relación a delitos graves que determinará en su derecho interno” por “en relación a los artículos 6 y 16 de esta Convención”

Rationale:

Artículo 23, inciso 2, (ámbito de aplicación de las medidas procesales)

La redacción del artículo **artículo 23 (ámbito de aplicación de las medidas procesales)**, inciso segundo, claramente habilita a que la Convención sea aplicada a otros delitos penales que no estén comprendidos en el capítulo de criminalización.

Esta redacción amplia supone un riesgo de que las fuerzas y cuerpos de seguridad puedan aplicar medidas que interfieran gravemente en el derecho a la libertad de expresión de las personas para, por ejemplo, perseguir delitos menores o delitos penales relacionados con el contenido, que son inherentemente incompatibles con las obligaciones de los Estados en materia de derechos humanos. A su vez es incompatible con los estándares internacionales de proporcionalidad y necesidad en tanto habilita a que las autoridades penales apliquen medidas intrusivas que podrían lesionar gravemente el derecho a la privacidad de las personas.

En ese sentido, recomendamos la eliminación de los **incisos b y c, del inciso 2, artículo 23**, a fin de garantizar que las medidas procedimentales solo sean aplicadas a los delitos incluídos directamente por la Convención.

Artículo 24

El capítulo sobre medidas procedimentales penales contiene tres problemas principales: *(i)* introduce facultades de vigilancia altamente invasivas en sus **artículos 27 a 30**;[18] mientras el **artículo 24**: *(ii)* ofrece escuetos controles democráticos y salvaguardas esenciales contra su abuso; y *(iii)* se aplica solamente a este capítulo.

La relevancia de garantías efectivas en contra del abuso de medidas de vigilancia electrónica encubierta ha sido destacada por la Asamblea General de la Organización de las Naciones Unidas,[19] el Relator Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión,[20] la Alta Comisionada para los Derechos Humanos de la ONU,[21] la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos[22], así como por organizaciones de la sociedad civil y expertos que han recogido las mejores prácticas derivadas de la jurisprudencia y doctrina comparada y han elaborado los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[23]

---

[18] Por ejemplo, el artículo 28 contempla el registro e incautación de datos informáticos almacenados, incluidos los dispositivos personales, mismos que contienen una gran cantidad de información personal sobre la persona. De igual forma, el artículo 29 prevé la obtención en tiempo real de datos relativos al tráfico, mismos que representan datos personales sensibles que pueden revelar patrones de movimiento, comunicación, relaciones, actividades y hábitos de navegación.
Por su parte, el artículo 30 establece la facultad para "autoridades competentes" de obtener o grabar datos relativos a contenido en tiempo real "*en relación con diversos delitos graves que determinará en su derecho interno*", sin supeditarse a ciberdelitos y dejando un peligroso márgen de acción para que ciertos Estados incluyan expresiones válidas en ejercicio de la libertad de expresión. También exige la cooperación confidencial de los proveedores de servicios para ayudar en la recopilación o grabación de datos.

[19] Asamblea General de la Organización de las Naciones Unidas. Resolución A/RES/68/167 sobre el derecho a la privacidad en la era digital. 18 de diciembre de 2013.

[20] ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue. 17 de abril de 2013. A/HRC/23/40, párr. 81: "La legislación debe estipular que la vigilancia estatal de las comunicaciones debe ocurrir únicamente bajo las circunstancias más excepcionales y exclusivamente bajo la supervisión de una autoridad judicial independiente. Las salvaguardas deben ser articuladas en la ley en relación a la naturaleza, alcance y duración de las posibles medidas, los motivos necesarios para ordenarlas, las autoridades competentes para autorizar, llevar a cabo y supervisarlas, y el tipo de recursos previstos en la ley para obtener una reparación". (Traducción propia)

[21] OACNUDH, *El derecho a la privacidad en la era digital*, 30 de Junio de 2014, A/HRC/27/37, párr. 37. El artículo 17, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos establece que toda persona tiene derecho a la protección de la ley en contra de interferencias o ataques ilegales o arbitrarios. La "protección de la ley" debe ser otorgada a través de salvaguardas procesales efectivas, incluyendo arreglos institucionales efectivos y financiados adecuadamente. Es claro, sin embargo, que la falta de supervisión efectiva ha contribuido a una falta de rendición de cuentas por intrusiones arbitrarias o ilegales en el derecho a la privacidad en el entorno digital. Salvaguardas internas, sin monitoreo independiente externo, han demostrado ser particularmente inefectivas contra métodos de vigilancia ilegales o arbitrarios. Mientras estas salvaguardas pueden tomar una variedad de formas, el involucramiento de todos los niveles de gobierno en la supervisión de programas de vigilancia, al mismo tiempo que una supervisión por parte de una agencia civil independiente, es esencial para asegurar una efectiva protección de la ley. (traducción propia)

[22] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

[23] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text

Artículo 24. Párrafo 1

En muchas experiencias latinoamericanas, autoridades —muchas veces, sin las competencias legales para realizar medidas de vigilancia— motivan el uso de dichas medidas con base únicamente en vagas consideraciones de seguridad nacional o combate al terrorismo.[24]

La **Corte Interamericana de Derechos Humanos (CIDH)** ha señalado que en el contexto de medidas de vigilancia encubierta, la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones, circunstancias y procedimientos en los que las autoridades estarán facultadas para recurrir a dichas medidas.[25]

Para que las restricciones a derechos tales como la privacidad, protección de datos personales y libertad de expresión cumplan con los estándares nacionales e internacionales en materia de derechos humanos, deben cumplir con los **requisitos de legalidad, necesidad y proporcionalidad**, lo cual implica el establecimiento de **salvaguardas adecuadas** para prevenir, evitar y remediar el ejercicio abusivo de las mismas.

En ese sentido, recomendamos que se modifique el primer párrafo del artículo para asegurar que los principios referidos anteriormente, salvaguardas como el control judicial, derecho a la notificación y medidas de transparencia, así como la perspectiva de género, deban ser incluidas tanto en el Convenio como en las legislaciones locales. En esta línea, notamos con preocupación que se excluyen las referencias a la obligación de proteger de forma adecuada los derechos humanos y las libertades, conforme a lo previsto en el Convenio de Budapest.

Artículo 24. Párrafo 2.

La redacción actual del **artículo 24, párrafo 2**, establece que las condiciones y salvaguardas establecidas estarán condicionadas "*en función de la naturaleza del procedimiento o la facultad de que se trate*". Esta redacción fomenta la discrecionalidad de los Estados y propicia el abuso de las medidas de vigilancia. La existencia de un estándar de necesidad o justificación de las medidas es indispensable para inhibir los riesgos de abuso de las medidas de vigilancia.

Las leyes que autoricen la aplicación de restricciones a nuestros derechos deben utilizar criterios precisos y no conferir una discrecionalidad sin controles a los encargados de su aplicación. Por lo que, recomendamos eliminar dicha expresión para aclarar que las condiciones y salvaguardias expresadas en este artículo se aplican a todos los

[24] Por ejemplo, en México se ha reportado la adquisición del *spyware* Pegasus por autoridades que no contaban con facultades para intervenir comunicaciones privadas, como lo ha sido la Secretaría de la Defensa Nacional. La evidencia recopilada deja como un hecho incontrovertible que dependencias del Estado mexicano contrataron y utilizaron Pegasus para espiar a periodistas, activistas, personas defensoras de derechos humanos, entre otros. De igual manera, se ha documentado la adquisición de licencias para el uso de *malware* de vigilancia comercializado por la empresa italiana Hacking Team por parte de múltiples autoridades sin facultades, como lo son la Secretaría de Gobierno del Estado de Jalisco, la Secretaría de Planeación y Finanzas del Gobierno de Baja California o incluso Petróleos Mexicanos.

[25] Corte IDH. *Caso Escher y otros vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200.

procedimientos o facultades previstos en el Convenio y son necesarias para una debida justificación del uso de las medidas procedimentales.

Salvaguardias

Recomendamos, en primer lugar, la necesidad de incluir los principios de legalidad, proporcionalidad y necesidad. Los Estados deben demostrar que cualquier restricción aplicada es necesaria y proporcionada al objetivo.

Por ejemplo, con respecto a las restricciones a la libertad de expresión, los mecanismos de la ONU han sostenido que "*el principio de necesidad y proporcionalidad presume que las restricciones no pueden justificarse cuando el daño a la libertad de expresión es mayor que los beneficios*".[26] Asimismo, la Corte IDH ha reconocido, al evaluar la necesidad de una limitación al derecho a la libertad, que *necesario* significa que los medios elegidos "*son absolutamente indispensables para alcanzar el fin perseguido, y que entre todas las medidas posibles, no existe ninguna menos severa en relación con el derecho involucrado, que sea tan adecuada para alcanzar el objetivo propuesto*".

En segundo lugar, consideramos crucial el establecimiento de salvaguardas adecuadas para prevenir, evitar y remediar el ejercicio abusivo de las medidas procedimentales previstas en el capítulo.

Por un lado, proponemos lineamientos específicos referentes al procedimiento de **control judicial** como elemento esencial para evitar que el abuso de poder mediante los Estados, considerando especialmente el contexto regional donde persiste evidencia del uso de medidas de vigilancia sin control judicial[27] e incertidumbre jurídica respecto de la necesidad imperiosa de control judicial previo o inmediato para llevar a cabo dichas medidas de vigilancia.[28] Dicho control judicial independiente no puede sustituirse por otros tipos de revisión independiente. En esta línea, el texto debe aclarar qué medidas procesales deben ser ineludiblemente autorizadas por una autoridad judicial antes de su aplicación y cuáles sólo pueden ser objeto de una revisión posterior, pero oportuna.

---

[26] Idem

[27] Por ejemplo, en México, entre 2016 y 2019, alrededor del 60 por ciento de las solicitudes de acceso a datos retenidos se realizaron sin supervisión judicial. Este porcentaje incluye tanto las solicitudes realizadas sin autorización judicial como las realizadas a través de mecanismos de emergencia. Alrededor del 75 por ciento de las solicitudes sin autorización judicial previa se realizaron a través de mecanismos de emergencia, y alrededor del 50 por ciento de estas solicitudes no fueron ratificadas o solo lo fueron parcialmente.
Respecto de lo anterior, no existe evidencia de que en esos casos las autoridades a las que de manera sistemática no le son ratificadas las medidas de vigilancia enfrenten algún proceso disciplinario ni que las personas afectadas sean notificadas de que su privacidad fue invadida de manera injustificada.

[28] La relevancia fundamental del control judicial previo o inmediato de medidas de vigilancia encubierta que invaden la privacidad de las personas ha sido resaltada por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la cual ha señalado que:

> Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover. *CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 165.*

Por otro lado, el hecho de que la mayoría de estas medidas se lleven en secrecía hace particularmente importante el **derecho de notificación** a la persona usuaria afectada como salvaguarda fundamental para proteger el derecho a la vida privada, garantizar el debido proceso y el acceso a un recurso efectivo. Este derecho establece la obligación de parte de la autoridad de notificar a una persona que su privacidad o datos personales fueron interferidos mediante una medida de vigilancia encubierta.[29]

Finalmente, es necesario establecer **mecanismos de transparencia** de manera que queden asentadas de manera pormenorizada e inmutable las medidas de vigilancia encubierta. En los casos de abuso de medidas de vigilancia persisten muchos obstáculos para el esclarecimiento de los casos, la rendición de cuentas y la reparación de las víctimas. Los registros fehacientes respecto de la adquisición y uso de herramientas de vigilancia son una herramienta eficaz para evitar estos obstáculos.

Artículos 29 y 30:

Bajo los mismos argumentos referentes a la necesidad de limitar el alcance de la Convención para evitar que ésta sea utilizada de manera abusiva o arbitraria, proponemos incluir la referencia de que dichos artículos serán aplicados únicamente a los delitos incluidos en los artículos 6 a 16 de la Convención.

Esto es especialmente importante considerando el carácter sumamente intrusivo de las facultades otorgadas en los artículos en cuestión. Desde una perspectiva de género, también es importante tener en cuenta que existe un riesgo significativo de uso excesivo o indebido de los poderes de aplicación de la ley en virtud de este capítulo del documento de negociación consolidado para recopilar datos sobre una amplia gama de personas o comunidades vulnerables o de alto riesgo. Las mujeres y otros grupos marginados se ven afectados por ello de forma más grave debido a su posición en la sociedad, exponiendo información sensible relativa a la salud personal, la sexualidad y las identidades y expresiones de género. Estas disposiciones podrían utilizarse, por ejemplo, para controlar los datos de localización y/o el uso de aplicaciones de seguimiento de la fertilidad por parte de personas que puedan quedarse embarazadas, con el fin de determinar la proximidad a los servicios de salud sexual y reproductiva.

4. **Cooperación internacional (Capítulo V)**

Recomendaciones:

Artículo 35: eliminar la referencia al artículo 17 y agregar el requisito de doble criminalidad para poder llevar adelante la cooperación internacional.

Artículo 36:

- Las salvaguardas establecidas en las medidas procedimentales también deben ser aplicables a las medidas de cooperación internacional, en especial en la transferencia de datos personales.

[29] Si bien dicha notificación puede no llevarse a cabo de manera previa o inmediata, en tanto se podría frustrar el éxito de una investigación, sí debe realizarse cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento pueda generar un riesgo inminente de peligro a la vida o integridad personal de alguna persona.

- Incluir la mención expresa al derecho internacional de los derechos humanos y a la perspectiva de género: "Los Estados partes no estarán obligados a transmitir datos personales en cumplimiento de la presente Convención si, *de conformidad con sus leyes y el derecho internacional de los derechos humanos aplicables bajo una perspectiva de género* en materia de protección de datos personales, no les está permitido hacerlo". Además, se sugiere agregar lo siguiente: “las normas mínimas de protección de datos basadas en los derechos humanos, como los principios de tratamiento lícito y justo, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad, no les está permitido hacerlo.”
- Tomar en consideración los riesgos relacionados con el género en la protección de datos personales.

Rationale:

La principal preocupación del apartado de cooperación internacional es la falta de salvaguardas en las facultades de asistencia legal y técnica mutua que se le dan a los Estados.

El apartado de cooperación internacional debe señalar que el **Artículo 24**, de la presente Convención también aplica al capítulo de cooperación internacional, de manera que se homologue la aplicación de dichas salvaguardas como criterio mínimo y esencial, independientemente de la jurisdicción en donde se estén llevando a cabo dicha medidas de vigilancia.

Artículo 35. Principios generales de cooperación internacional

Conforme hemos referido en apartados anteriores, es esencial que el alcance de la Convención sea limitado a los delitos reconocidos en los artículos 6 a 16. Al eliminar la referencia al artículo 17, se provee un marco legal claro para la cooperación internacional asegurando que la Convención no sea utilizada en detrimento de los derechos de libertad de expresión y asociación, entre otros.

En cuanto al principio de doble criminalidad como un requisito para la cooperación internacional, es necesario que sea incluido como una obligación para garantizar que la cooperación no sea solicitada por motivos políticos, de discriminación basada en género y/o arbitrarios. Bajo una perspectiva de género, es importante considerar que en muchos países la identidad de género, la orientación sexual y/o el aborto son cuestiones que se encuentran penalizadas, generando graves riesgos de vigilancia y criminalización para mujeres y personas pertenecientes al colectivo LGTBIQ.

Artículo 36. Protección de datos personales

El artículo solamente menciona el derecho interno aplicable en materia de protección de datos personales como excepción a la obligación de transmitir datos personales.

Esta previsión es insuficiente debido a que la protección de los datos personales es un derecho, junto con el derecho a la privacidad, que es reconocido por el derecho internacional de los derechos humanos y marcos jurídicos regionales como el Sistema

Interamericano. Esto es especialmente importante al considerar que no todos los países cuentan con legislaciones de datos personales.

Recomendamos incluir la mención expresa al derecho internacional de los derechos humanos bajo una perspectiva de género y hacer referencia a estándares internacionales específicos dentro del primer párrafo del Artículo 36. De esta forma se sugiere agregar lo siguiente: Los Estados partes no estarán obligados a transmitir datos personales en cumplimiento de la presente Convención si, de conformidad con sus leyes aplicables en materia de protección de datos personales y las normas mínimas de protección de datos basadas en los derechos humanos con perspectiva de género, como los principios de tratamiento lícito y justo, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad, no les está permitido hacerlo.

El texto señala que únicamente las salvaguardias efectivas del derecho interno son aplicables a la transferencia de datos personales entre Estados. De igual forma, el texto establece de manera ambigua la obligación de los Estados de aplicar estas salvaguardas. Esto debido a que el verbo “velarán” puede ser interpretado como una opción o facultad potestativa, en vez de la obligación expresa que tienen los Estados de proteger el derecho a la privacidad y protección de datos personales.

Recomendamos que el texto señale que las salvaguardas del **artículo 24** son aplicables a todas las medidas de cooperación internacional, incluyendo las que estén relacionadas con la transferencia de datos personales.

El capítulo de cooperación internacional debe aplicar la perspectiva de género. Esta perspectiva se implementa al analizar los impactos diferenciados de género que presenta la recopilación de datos para las comunidades en situación de vulnerabilidad o de alto riesgo. Para asegurar la protección de los derechos de estas comunidades deben de incluirse salvaguardias de protección diferenciada.

La recopilación de datos nunca tiene lugar en un entorno neutro desde el punto de vista del género. Es crucial que la recopilación, almacenamiento y transferencia de datos esté sujeto a un análisis interseccional de género para identificar los riesgos para la seguridad individual que dichos procedimientos conllevan. Por ejemplo, los amplios poderes para intercambiar datos entre Estados puede ser problemático para personas con identidades, expresiones y orientaciones sexuales diversas, tanto en general como en jurisdicciones donde la expresión de identidades LGBTQIA+ no están actualmente permitidas legalmente y/o para mujeres/personas gestantes en jurisdicciones donde el acceso al aborto está prohibido, generando grandes riesgos de criminalización y vigilancia.

En ese sentido, como ya hemos señalado en apartados anteriores, es imperativo que en se agregue que se debe aplicar la la perspectiva de género dentro del marco a considerar de derechos humanos entendiendo que cuestiones de género -incluidas la sexualidad, la identidad de género y la expresión de género- son datos personales privados que requieren una protección especial.

Las recomendaciones formuladas se ajustan a las resoluciones de la ONU en materia de privacidad. En ejemplo, la última[30] hace hincapié en que los Estados deben respetar obligaciones internacionales de derechos humanos relativas al derecho a la intimidad cuando recojan datos personales, cuando compartan o faciliten de otro modo el acceso a la recopilación de datos a través de, entre otros información e inteligencia, y cuando exijan la divulgación de datos personales a terceros, incluidas las empresas.

Presentado por ONG registradas bajo el operativo 8 o 9:

Derechos Digitales
Red en Defensa de los Derechos Digitales (R3D)
Instituto Panamericano de Derecho y Tecnologías (IPANDETEC)
Hiperderecho

La lista completa de firmantes que apoyan esta sumisión está disponible en este enlace.

[30] Asamblea General. A/RES/77/211. Resolución adoptada por la Asamblea General en 15 Diciembre 2022. El derecho a la privacidad en la era digital (p. 5). https://www.undocs.org/A/RES/77/211

Anexo 1 - Propuestas de texto

Incorporar la perspectiva de género en toda la convención en su conjunto y a través de cada artículo en los esfuerzos para prevenir y combatir la ciberdelincuencia.

Capítulo I Disposiciones generales

Artículo 5. Respeto de los derechos humanos

Los Estados partes velarán por que el cumplimiento de sus obligaciones con arreglo a la presente Convención se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos, el principio de igualdad y no discriminación y la igualdad de género.

Capítulo II Criminalización

Artículo 6. Acceso ilícito

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el acceso deliberado y con intención maliciosa ~~sin derecho~~ a la totalidad o una parte de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones].

2. Los Estados partes podrán exigir como requisito que el delito se cometa infringiendo las medidas de seguridad, con la intención dolosa de obtener [datos informáticos] [información digital] o con otra intención maliciosa ~~deshonesta,~~ en relación con un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] que esté conectado a otro [sistema informático] [dispositivo de tecnología de la información
y las comunicaciones].

3.Los Estados Parte deberán exigir como requisito que los actos descritos en el párrafo 1 y 2 resulten en daños graves.

Artículo 8. Interferencia con [datos informáticos] [información digital]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado y con intención maliciosa ~~derecho~~ que dañe, borre, deteriore, altere o suprima [datos informáticos] [información digital].
2.Los Estados Parte deberán exigir como requisito que los actos descritos en el párrafo 1 comporten daños graves.

Artículo 9. Interferencia con un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada y con intención maliciosa ~~sin derecho~~ del funcionamiento de un [sistema

informático] [dispositivo de tecnología de la información y las comunicaciones] mediante la introducción ,transmisión, daño, borrado, deterioro, alteración o supresión d e [datos informáticos]
[información digital]

2.Los Estados Parte deberán exigir como requisito que los actos descritos en el párrafo 1 comporten daños graves.

Capítulo IV Medidas Procesales y aplicación de la Ley

Artículo 24 Condiciones y salvaguardias

1. Cada Estado parte se asegurará de que la instauración, ejecución y aplicación de las facultades y procedimientos previstos en el presente capítulo se sometan a las condiciones y salvaguardias definidas previstas en su derecho interno, que deberán ser acordes con las obligaciones que haya asumido en virtud del derecho internacional de los derechos humanos bajo una perspectiva de género y que deberán integrar, **como mínimo**, **los** principio**s** de **legalidad, necesidad y** proporcionalidad, **garantizando el derecho a la privacidad, protección de datos e incorporando una perspectiva de género y con base en requisitos de procedencia objetivos y verificables que justifiquen el ejercicio de dichas facultades.**

2. Dichas condiciones y salvaguardias deberán incluir, ~~cuando proceda en función de la naturaleza del procedimiento o la facultad de que se trate, incluirán una revisión judicial u otra forma de revisión independiente, los motivos que justifiquen su aplicación y la limitación del alcance y la duración de dicha facultad o procedimiento~~, entre otras cosas:

a) Procedimientos para una autorización judicial independiente y previa para las medidas referidas en los artículos 27 a 31, y una revisión judicial expedita de las medidas referidas en los artículos 25 y 26.

b) La obligación de mantener registros detallados de las medidas implementadas. Los registros deben ser accesibles para las autoridades encargadas de investigar el potencial uso ilegal o abusivo de dichas medidas procedimentales.

c) La obligación de las autoridades facultadas para ejercer cualquiera de las facultades y procedimientos previstos en este capítulo, y de cualquier prestador de servicios que asista en cualquier manera en la implementación de las medidas procedimentales, de producir un reporte anual de transparencia que revele, como mínimo, información estadística desagregada con respecto al número de medidas implementadas, autorizadas o rechazadas; así como el número de personas, cuentas o dispositivos afectados por dichas medidas.

d) La notificación de cualquier persona cuyos datos personales están sujetos a las medidas procedimentales previstas en este capítulo. La notificación puede demorarse sin previa autorización judicial independiente por un periodo máximo de un año después de que la medida procedimental comenzó a ser implementada.

e) El establecimiento de un órgano de supervisión independiente autorizado para auditar de manera aleatoria la implementación de las medidas procedimentales.

3. ~~Siempre que sea conforme con el interés público, y en particular con la debida administración de justicia, cada Estado parte examinará los efectos de las facultades y procedimientos mencionados en el presente artículo sobre los derechos, responsabilidades e intereses legítimos de terceros.~~

Los poderes y procedimientos en este capítulo no deben construirse con el alcance de requerir que ninguna persona o proveedor de servicios comprometa la seguridad o integridad de sus servicios o para que genere riesgos significativos en terceros.

Artículo 29: Obtención en tiempo real de datos relativos al tráfico

1. Respecto a los tipos penales establecidos de conformidad con los artículos 6 a 16 de la presente Convención, cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a:

(...)

Artículo 30. Interceptación de datos relativos al contenido

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias, respecto a los tipos penales establecidos de conformidad con los artículos 6 a 16 de la presente Convención, para facultar a sus autoridades competentes a:

(...)

Capítulo V Cooperación internacional

Artículo 35 Principios generales de la cooperación internacional

1. Los Estados partes cooperarán entre sí de conformidad con lo dispuesto en la presente Convención, así como en otros instrumentos internacionales aplicables en materia de cooperación internacional en asuntos penales, y en su derecho interno, a efectos de las investigaciones, acciones penales y procesos judiciales relativos a los delitos tipificados con arreglo a los artículos 6 a 16 de la presente Convención, o para la reunión, obtención, conservación e intercambio de pruebas en formato electrónico de los delitos tipificados con arreglo a los artículos 6 a 16 de la presente Convención, así como de los delitos graves, ~~incluidos los delitos contemplados en el artículo 17 de la presente Convención~~. Esta cooperación está supeditada, en todos los casos, al cumplimiento del principio de doble incriminación.

Artículo 36

(primer párrafo) (....) Los Estados partes no estarán obligados a transmitir datos personales en cumplimiento de la presente Convención si, *de conformidad con sus leyes y el derecho internacional de los derechos humanos aplicables, como los principios de tratamiento lícito y justo, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad, no les está permitido hacerlo.*

"2. En lo que respecta a los datos personales transmitidos de conformidad con la presente Convención, los Estados partes ~~velarán~~ *deberán asegurarse* que los datos personales recibidos estén sujetos a *las* salvaguardias efectivas y adecuadas *establecidas en la presente Convención, en el derecho internacional de los derechos humanos y en* sus respectivos marcos jurídicos".

Artículo 40. Principios generales y procedimientos relativos a la asistencia judicial recíproca

21. Se podrá denegar la asistencia judicial recíproca:

a) cuando la solicitud no se haga de conformidad con lo dispuesto en el presente artículo; b) cuando el Estado parte requerido considere que el cumplimiento de lo solicitado podría menoscabar su soberanía, su seguridad, su orden público u otros intereses fundamentales;
c) cuando el derecho interno del Estado parte requerido prohíba a sus autoridades actuar de la forma solicitada con respecto a un delito análogo, si este hubiera sido objeto de investigaciones, acciones penales o procesos judiciales en el ejercicio de su propia competencia;
d) cuando acceder a la solicitud sea contrario al ordenamiento jurídico del Estado parte requerido en lo relativo a la asistencia judicial recíproca
e) *cuando la ejecución de la solicitud pueda perjudicar, entre otras cosas, la protección de los derechos humanos o las libertades fundamentales y la igualdad de género.*

Capítulo VII Asistencia técnica e intercambio de información

Artículo 54. Asistencia técnica y fomento de la capacidad

3. Las actividades a que se refieren los párrafos 1 y 2 del presente artículo podrán incluir, en la medida en que lo permita el derecho interno, las siguientes:

a) métodos y técnicas empleados en la prevención, la detección, la investigación y el enjuiciamiento de los delitos contemplados en la presente Convención;

b) *métodos para integrar la perspectiva de género en la elaboración de políticas, la legislación y la planificación*

c) fomento de la capacidad para formular y planificar políticas estratégicas y leyes destinadas a prevenir y combatir [la ciberdelincuencia] [los delitos cometidos mediante la utilización de tecnologías de la información y las comunicaciones];

d) fomento de la capacidad para recabar, conservar y transmitir pruebas, en particular en formato electrónico, incluido el mantenimiento de la cadena de custodia y el análisis forense;

e) equipo moderno para la aplicación de la ley y utilización de ese equipo;

f) capacitación de las autoridades competentes respecto de la preparación de solicitudes de asistencia judicial recíproca y otros medios de cooperación que cumplan los requisitos establecidos en la presente Convención, especialmente para la obtención, conservación y transmisión de pruebas en formato electrónico;

g) prevención, detección y vigilancia del traslado del producto de delitos contemplados en la presente Convención o de los bienes, el equipo u otros instrumentos y de los métodos empleados para la transferencia, ocultación o disimulación de dicho producto, bienes, equipo u otros instrumentos;

h) mecanismos y métodos jurídicos y administrativos apropiados y eficientes para facilitar la incautación y la restitución del producto de delitos contemplados en la presente Convención;

i) métodos utilizados para proteger a las víctimas y los testigos que cooperen con las autoridades judiciales;

j) capacitación sobre derecho sustantivo y procesal pertinente y sobre facultades de investigación para la aplicación de la ley, así como sobre normativa nacional e internacional e idiomas.