ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Trámite Legislativo
2024 - 2029

Código AN_SG_10
Versión 0
Fecha de versión 7-may-2024

		PERIODO LEGISLATIVO	2024 - 2025
Anteproyecto de Ley N°		Proyecto de Ley N°	61
Ley N°		Gaceta Oficial	
Etapa	PENDIENTE DE SANCIÓN		

INFORMACIÓN GENERAL

Fecha de Presentación	05-sep-24	Comisión	GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES
Título	POR EL CUAL SE ADOPTAN MEDIDAS CONTRA LA CIBERDELINCUENCIA Y SE DICTAN OTRAS.		
Proponente:	S.E. Javier E. Caraballo Salazar, Procurador General de la Nación		

DEBATES

Fecha de Prohijamiento	
Fecha de I Debate	05-sep-24
Fecha de II Debate	08-oct-24
Fecha de III Debate	09-oct-24

Observaciones:	Proyecto de Ley N°61 fusionado con los Proyectos N°45 y N°50, Prevalece el Numero 61

PROYECTO DE LEY Nº0061
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

República de Panamá
Procuraduría General de la Nación

Panamá, 4 de septiembre de 2024
Nota PGN-FSL-147-2024

Honorable Diputada
Dana Castañeda
Presidenta de la Asamblea Nacional
E. S. D.

Señora Presidenta:

En uso de la iniciativa legislativa que me confiere el artículo 165 de la Constitución Política de la República de Panamá, presento por su conducto al Pleno de este Órgano del Estado, el Proyecto de Ley **"Por el cual se adoptan medidas contra la Ciberdelincuencia"**, el cual amerita las siguientes consideraciones:

EXPOSICIÓN DE MOTIVOS

En ejercicio de la atribución constitucional contemplada en el literal c del numeral 1 del artículo 165 de la Constitución Política, para presentar proyectos de leyes siempre que se trate de la expedición o reformas de los Códigos Nacionales, someto a la consideración de los Honorables Diputados de la Asamblea Nacional, el Proyecto de Ley **"Por el cual se adoptan medidas contra la Ciberdelincuencia".**

I. Introducción

La ciberdelincuencia es una realidad global en constante evolución que afecta tanto a individuos como a organizaciones, públicas y privadas. El crecimiento exponencial de delitos cometidos a través de medios tecnológicos, como fraudes informáticos, accesos ilícitos a sistemas y la distribución de material de abuso sexual infantil en línea, ha revelado la urgente necesidad de una respuesta jurídica sólida y coordinada a nivel internacional.

En Panamá, de acuerdo a las estadísticas plasmadas en el informe de la marcha sobre la administración de justicia, se produjo un aumento de un 113% en los delitos contra la seguridad informática, en el período de junio 2023 a mayo de 2024, en comparación con el

período anterior, junio 2022 a mayo de 2023, lo cual refleja un incremento sustancial en diversas conductas punibles como el acceso ilícito a base de datos, red o sistema informático; apoderamiento, modificación y utilización indebida de base de datos, entre otras conductas que afectan gravemente al sector público y generan pérdidas económicas para la empresa privada.

En este contexto, el Convenio de Budapest sobre Ciberdelincuencia, adoptado por el Consejo de Europa en 2001 y aprobado por la República de Panamá mediante la Ley 79 del 22 de octubre de 2013, se ha consolidado como el principal instrumento jurídico internacional en la lucha contra los delitos cibernéticos, instando a los Estados a adoptar medidas legislativas para que el catálogo de conductas punibles descritas sea incluido en el derecho interno. Además de establecer, en el derecho procesal, los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como implementar un régimen rápido y eficaz de cooperación internacional.

Por su parte, la Asamblea General de las Naciones Unidas, el 9 de agosto de 2024, adoptó el Proyecto de Convención de las Naciones Unidas contra la Ciberdelincuencia, un documento que fortalecerá la capacidad de los Estados para prevenir y reprimir la ciberdelincuencia, especialmente a través de la cooperación internacional y la transmisión electrónica de pruebas. Aunque este documento aún no ha sido firmado ni ratificado, representa el resultado de varios años de trabajo del Comité Especial encargado de su redacción. En este proceso, las autoridades panameñas jugaron un papel crucial mediante la participación del equipo interinstitucional, conformado por la Procuraduría General de la Nación, la Autoridad Nacional para la Innovación Gubernamental y el Ministerio de Relaciones Exteriores.

II. Necesidad de Adecuación Legislativa

El avance tecnológico tiene un impacto indudable en el ámbito penal, donde se vuelve imprescindible adecuar las tipificaciones delictivas a las nuevas realidades cibernéticas, que abarcan una amplia gama de delitos, tanto tradicionales, en los que se utilizan medios tecnológicos para su comisión, como otros que se enfocan en la vulneración de sistemas informáticos y la evasión de controles establecidos. Muchas de estas conductas actualmente quedan impunes debido a la falta de regulación adecuada en la normativa vigente.

Ante este escenario, la Procuraduría General de la Nación considera prioritario redoblar los esfuerzos para contar con una legislación robustecida con herramientas jurídicas que

nos permitan afrontar los retos y superar los obstáculos en materia de investigación, además garantizar una cooperación internacional más efectiva, en materia de ciberdelincuencia.

De esta forma, se conformó un equipo de fiscales especializados, para la elaboración del presente proyecto de ley, el cual tiene como objetivo principal la adecuación de la legislación nacional al Convenio de Budapest, así como la incorporación de las tendencias modernas en la lucha contra la ciberdelincuencia. Este equipo contó con el apoyo de personal experto en la materia del Consejo de Europa, con el fin de tener una orientación jurídica sobre el alcance de los tipos penales precisos, fortaleciendo con ella la visión nacional en beneficio de la capacidad del Estado para enfrentar los desafíos que plantea la investigación de estas conductas.

Dicha adecuación no solo responde a las obligaciones internacionales asumidas por el Estado, sino que también se convierte en una herramienta esencial para proteger los derechos fundamentales de los ciudadanos en un entorno cada vez más digitalizado. La seguridad en el ciberespacio, el respeto a la privacidad y la protección de datos personales son derechos que deben ser garantizados mediante normas modernas y eficaces.

III. Aspectos sustantivos de la Lucha contra la Ciberdelincuencia

La ciberdelincuencia es un concepto complejo que abarca una amplia gama de actividades ilícitas que tienen como objetivo las Tecnologías de la Información y la Comunicación (TIC) o que las utilizan para la comisión de delitos. Los ciberdelitos se dividen en dos categorías principales: aquellos facilitados por la cibernética y aquellos basados en ella.

Los delitos facilitados por la cibernética son aquellas conductas tradicionales que se ven potenciadas por el uso de las Tecnologías de la Información y la Comunicación (TIC). En estos casos, las tecnologías juegan un papel fundamental en el modus operandi del delincuente. Por otro lado, los delitos basados en la cibernética son aquellos que solo pueden cometerse mediante el uso de computadoras, redes informáticas u otras formas de tecnología de la información, donde el objetivo principal del delito es precisamente vulnerar los sistemas informáticos.

Este proyecto de ley introduce nuevos tipos penales específicos para conductas delictivas que no estaban contempladas en la legislación vigente, tales como el abuso de dispositivos, la interceptación ilícita de datos, los ataques a la integridad de los sistemas, el acoso de menores por vías cibernéticas, la suplantación de identidad, la difusión no consentida de material íntimo, entre otros delitos relevantes. Asimismo, se ajusta el concepto de "pornografía

infantil" al término más preciso de "material de abuso sexual infantil," en línea con las tendencias modernas y los estándares internacionales.

IV. Herramientas de Investigación y Procedimientos Penales

Para enfrentar la creciente sofisticación y complejidad de los delitos cibernéticos, es esencial que las autoridades competentes cuenten con herramientas adecuadas de investigación. En este sentido, el proyecto de ley propone la inclusión de un capítulo específico que regule la evidencia digital, abarcando aspectos cruciales como su preservación y la obtención en tiempo real de datos relativos al tráfico o al contenido.

Estas medidas son indispensables para garantizar la integridad y disponibilidad de las pruebas en un entorno digital donde la información puede ser fácilmente alterada o destruida. La regulación clara y precisa de la evidencia digital es clave para asegurar que las investigaciones cibernéticas sean efectivas y robustas, protegiendo así los derechos procesales y fortaleciendo la lucha contra la ciberdelincuencia.

V. Cooperación Internacional

De igual forma, el proyecto de ley busca facilitar la asistencia mutua en la investigación y persecución de delitos cibernéticos, promoviendo el intercambio de información y la ejecución de órdenes judiciales provenientes del extranjero. Dado el carácter transfronterizo de la ciberdelincuencia, es fundamental contar con mecanismos de cooperación internacional efectivos y ágiles.

Para ello, se proponen una serie de modificaciones que incluyen la obtención de elementos de convicción y pruebas en formato electrónico de un delito, así como la promoción de la participación activa en redes permanentes de cooperación internacional, como la Red 24/7 del Convenio de Budapest. Esta red permite a las autoridades nacionales solicitar y recibir asistencia urgente en la investigación de delitos cibernéticos en cualquier momento, fortaleciendo así la capacidad del Estado para responder a las amenazas cibernéticas con rapidez y eficacia.

VI. Conclusión

La adecuación de la legislación interna al Convenio de Budapest no solo responde a las necesidades actuales de la lucha contra la ciberdelincuencia, sino que también reafirma el compromiso del Estado con la protección de los derechos fundamentales en el ciberespacio.

Este proyecto de ley constituye un paso decisivo hacia una mayor seguridad y justicia en el entorno digital, al tiempo que fortalece la cooperación internacional en la persecución de delitos que trascienden nuestras fronteras.

En un mundo cada vez más interconectado, disponer de herramientas jurídicas modernas y eficaces es esencial para garantizar la protección de la sociedad frente a las amenazas del ciberespacio. Por ello, insto a la pronta aprobación de este proyecto de ley, en beneficio de la seguridad, la justicia y el bienestar de todos los ciudadanos.

Tomando en cuenta las consideraciones precedentes y las decisiones legislativas orientadas a mejorar las herramientas del sistema de justicia penal, presento este Proyecto de Ley.

Javier E. Caraballo Salazar
Procurador General de la Nación

PROYECTO DE LEY N°___

De ___ de septiembre de 2024

Por el cual se adoptan medidas contra la Ciberdelincuencia y se dictan otras disposiciones

LA ASAMBLEA NACIONAL,

DECRETA:

Artículo 1. A los efectos de la presente Ley los términos a continuación tendrán el siguiente significado:

1. Sistema informático. Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
2. Datos informáticos. Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
3. Proveedor de servicios:
    a. Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático; y,
    b. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.
4. Datos relativos al tráfico. Todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.
5. Datos relativos a los abonados. cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:
    a. El tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b. La identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio; y,
c. Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

6. Datos relativos al contenido. Se entiende el contenido comunicativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o la información transmitida por la comunicación. Se trata de todo lo transmitido como parte de la comunicación que no sean datos relativos al tráfico.
7. Infraestructura crítica. Las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
8. Material de abuso sexual infantil. Comúnmente denominado pornografía infantil, se entiende cualquier representación, por cualquier medio, de un menor participando en actividades sexuales explícitas, reales o simuladas, o cualquier representación de los órganos sexuales de un menor para fines principalmente sexuales, además del uso de un menor para crear tal representación.

Artículo 2: Se adiciona el artículo 166-A al Código Penal, así:

Artículo 166-A: Quién, con la intención de causar daño, sin el consentimiento expreso de su titular, publique o difunda al público en general o a terceros en particular, de forma deliberada, a través de tecnologías de la información y comunicación electrónica, contenido multimedia sexual explícito, producido en un ámbito de intimidad, será sancionado con uno a tres años de prisión.

La pena se aumentará de una sexta parte a la mitad cuando las conductas descritas en el párrafo anterior se cometen con fines lucrativos o cuando el autor se apodere u obtenga indebidamente dicho contenido.

Artículo 3. El artículo 184 del Código Penal, queda así:

Artículo 184. Quien fabrique, elabore por cualquier medio o produzca material de abuso sexual infantil o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de un medio de transferencia de datos, sistema informático, datos

informáticos, programas maliciosos o cualquier tecnología emergente o cualquier medio de comunicación o información nacional o internacional, presentando o representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de diez a quince años.

La pena será de quince a veinte años de prisión si la víctima es una persona menor de catorce años o personas con capacidades especiales, si el autor pertenece a una organización criminal nacional o internacional o si el acto se realiza con ánimo de lucro.

Artículo 4: Se adiciona el artículo 184-A al Código Penal, así:

Artículo 184-A. Quien, con la finalidad de cometer delitos Contra la Libertad e Integridad Sexual, utilice cualquier medio, inclusive un sistema informático, sistema electrónico o comunicación electrónica para contactarse o comunicarse con una persona menor de edad o persona con capacidades especiales que no le permita resistirse, será sancionado con pena de prisión de dos a cuatro años.

La pena será de cuatro a seis años de prisión si la víctima es una persona menor de catorce años.

Artículo 5. El artículo 185 del Código Penal, queda así:

Artículo 185. Quien posea para su propio uso material de abuso sexual infantil o que contenga la imagen, real o simulada, de personas menores de edad, voluntariamente adquirido, será sancionado con pena de prisión de cinco a diez años.

La pena será aumentada de una sexta parte a un tercio cuando se utilicen sistemas informáticos o medios de almacenamiento electrónico o redes sociales.

Artículo 6. Se adiciona el artículo 226-A al Código Penal, así:

Artículo 226-A. Quien suplante la identidad de una persona, para procurarse para sí o para un tercero un provecho ilícito, utilizando datos informáticos contenidos en una base de datos o un sistema informático, sistema electrónico, o adquiridos de cualquier otra forma, será sancionado con pena de dos a cuatro años de prisión.

Cuando la conducta cause un daño económico superior a los veinte mil balboas (B/. 20,000.00) la pena se aumentará a la mitad.

Artículo 7. Se adiciona el artículo 289-A al Código Penal, así:

Artículo 289-A. Quien, indebidamente, por medios técnicos, intercepte, interrumpa o interfiera datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, será sancionado con prisión de dos a cuatro años de prisión.

Artículo 8. El artículo 290 del Código Penal, queda así:

Artículo 290. Quien indebidamente se apodere, copie, utilice, modifique, dañe, borre, deteriore, altere o suprima datos informáticos, en tránsito o contenidos en una base de datos o sistema informático, será sancionado con dos a cuatro años de prisión.

Si la conducta descrita en el párrafo anterior causa un daño grave al titular de los datos informáticos la sanción se aumentará de un tercio a una sexta parte.

Artículo 9. Se adiciona el artículo 290-A al Código Penal, así:

Artículo 290-A. Quien indebidamente obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, será sancionado con dos a cuatro años de prisión.

Artículo 10. El artículo 291 del Código Penal, queda así:

Artículo 291. Las conductas descritas en éste Capítulo se agravarán de un tercio a una sexta parte de la pena si se cometen contra un sistema informático, sistema electrónico, datos informáticos de:

1. Oficinas públicas o bajo su tutela.
2. Instituciones públicas, privadas o mixtas que prestan un servicio público.
3. Bancos, aseguradoras y demás instituciones financieras y bursátiles.
4. Hospitales o cualquier tipo de entidad que maneje información relativa a datos médicos.

5. Sistemas informáticos o similares pertenecientes a infraestructura crítica o sistemas gubernamentales.

También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos con fines lucrativos o infringiendo medidas de seguridad.

Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV, del Libro Segundo de este Código.

Artículo 11. Se adiciona el artículo 292-A al Código Penal, así:

Artículo 292-A. Quien produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición cualquier dispositivo, incluido un programa informático, concebido o adaptado para la comisión de delitos a los que se refiere el presente capítulo, a sabiendas de su finalidad, será sancionado con dos a cuatro años de prisión.

Igual sanción se aplicará a quien obtenga o difunda una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con el fin de cometer delito.

No se considera delito la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el presente artículo que no tenga por objeto la comisión de uno de los delitos previstos en el Código Penal, ni tampoco la divulgación de datos informáticos o documentos indispensables para la comprensión de la historia, las ciencias, las artes o cualquier información que sea de interés público.

Artículo 12. Se adiciona el artículo 428-A al Código Penal, así:

Artículo 428-A. Quien suplante la identidad de una persona, con el fin de obtener información confidencial o de seguridad del Estado, la pena será de cuatro a seis años.

Artículo 13. El numeral 1 del artículo 112 del Código Procesal Penal, queda así:

Artículo 112. Acción pública dependiente de instancia privada. **...**

...

1. **Delitos de difusión no consentida de material íntimo**, acoso sexual y abusos deshonestos, cuando la víctima sea mayor de edad.

2. ...

Artículo 14. Se adiciona el artículo 314-A al Código Procesal Penal, así:

Artículo 314-A. Registro e incautación de datos informáticos almacenados. El Ministerio Público, en el marco de las investigaciones, podrá registrar o tener acceso a un sistema informático o a parte del mismo, así como incautar los datos informáticos en él almacenados.

En el caso en que tengan motivos para creer que los datos buscados se encuentran almacenados en otro sistema informático o en una parte del mismo, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, pueden extender el registro o el acceso de un modo similar al otro sistema.

En aplicación del presente artículo, se podrá obtener y conservar una copia de los datos informáticos y preservar su integridad. De ser necesario, se dispondrá hacerlos inaccesibles o suprimirlos en el sistema informático consultado.

Artículo 15. Se adiciona el Capítulo VI al Título I del Libro Tercero del Código Procesal Penal, así:

Capítulo VI
Evidencia Digital

Artículo 16. Se adiciona el artículo 338-A al Código Procesal Penal, así:

Artículo 338-A. Conservación rápida de datos informáticos almacenados. El Ministerio Público podrá ordenar, a cualquier persona natural o jurídica, la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, que se encuentren en su poder o bajo su control, así como la protección de su integridad, cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. Esta medida no podrá exceder de noventa días, prorrogables por igual término, siempre que se mantengan las condiciones que motivaron su disposición.

La persona que custodia los datos o quien se encuentre encargada de su conservación estará obligada a mantener la reserva de la ejecución de la medida.

Artículo 17: Se adiciona el artículo 338-B al Código Procesal Penal, así:

Artículo 338-B: Conservación y revelación rápida de los datos relativos al tráfico. El Ministerio Público podrá ordenar a los proveedores de servicios, que hayan participado en la transmisión, la conservación rápida de los datos relativos al tráfico.

Si el proveedor requerido advierte que, en la comunicación, objeto de la investigación, han participado otros proveedores, deberá revelar rápidamente los datos que permitan identificar a todos los proveedores de servicio como la vía por la cual se transmitió la comunicación.

Artículo 18. Se adiciona el artículo 338-C al Código Procesal Penal, así:

Artículo 338-C. Orden de suministro. El Ministerio Público podrá ordenar a una persona, natural o jurídica, que suministre datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; o a un proveedor que ofrezca sus servicios en el territorio nacional, que suministre los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

Cuando el Ministerio Público logre la obtención de los datos correspondientes someterá los mismos al control posterior del Juez de Garantías, de conformidad con las reglas establecidas en este Código para la incautación de datos.

Artículo 19. Se adiciona el artículo 338-D al Código Procesal Penal, así:

Artículo 338-D. Obtención en tiempo real de datos relativos al tráfico y al contenido. Para la obtención o grabación, en tiempo real, de datos relativos al tráfico o relativos al contenido, por medios tecnológicos, se procederá conforme a lo establecido en el artículo 311 de este Código.

Para ello se podrá ordenar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas, su colaboración y su asistencia, quien deberá mantener la reserva de la medida.

Artículo 20. El artículo 4 de la Ley 11 de 31 de marzo de 2015, queda así:

> **Artículo 4.** Cuando la solicitud de asistencia jurídica no tenga fundamento en un convenio bilateral o multilateral del que la República de Panamá sea parte y se sustente en el principio de reciprocidad entre las naciones, corresponderá al Ministerio de Relaciones Exteriores recibir y remitir las solicitudes de asistencia jurídica vía diplomática. La viabilidad de la solicitud de asistencia jurídica presentada por el Estado requirente será determinada por la Procuraduría General de la Nación.

Artículo 21. Se adiciona el numeral 5 al artículo 6 de la Ley 11 de 31 de marzo de 2015, queda así:

> **Artículo 6.** ...
>
> ...
>
> 5. La asistencia se brindará conforme al principio de la doble incriminación, con independencia de que dicha conducta delictiva no se encuentre dentro de la misma categoría de delitos o se le denomine con una terminología distinta.

Artículo 22. El artículo 7 de la Ley 11 de 31 de marzo de 2015, queda así:

> **Artículo 7.** La asistencia jurídica internacional podrá solicitarse para:
>
> 1. La recepción de entrevistas, testimonios o declaraciones.
> 2. La remisión de documentos legales.
> 3. El examen de documentos, objetos y lugares.
> 4. La facilitación de información, elementos de pruebas y evaluaciones periciales.
> 5. La entrega de originales o copias certificadas de los documentos y expedientes pertinentes, incluida la documentación pública, bancaria o financiera, así como la documentación social o comercial de sociedades.
> 6. La identificación o localización del producto del delito, los bienes o activos lavados, procedentes de los instrumentos usados o que se pretenden usar en un acto delictivo o para la financiación del terrorismo, los bienes de valor equivalente u otros elementos con fines probatorios.
> 7. La facilitación de la comparecencia voluntaria de las personas al Estado requirente.
> 8. La autorización de la presencia, durante la ejecución de una solicitud, de las autoridades competentes de la Parte requirente o de sus delegados oficiales.

9. La aprehensión, incautación, embargo o comiso de bienes muebles e inmuebles, dineros, títulos, valores, bienes o activos producto del delito, procedentes de instrumentos usados o que se pretenden usar en un acto delictivo o para la financiación del terrorismo y bienes de valor equivalente.
10. La realización de videoconferencias.
11. La entrega de antecedentes penales.
12. La búsqueda y localización de personas.
13. La realización de técnicas especiales de investigación como operaciones encubiertas, interceptación de comunicaciones, acceso a sistemas informáticos y entregas controladas.
14. La obtención de elementos de convicción y de pruebas de un delito en formato electrónico.
15. Otras formas de asistencia legal de conformidad con los fines de esta Ley, siempre que no sean incompatibles con las leyes nacionales.

Artículo 23. El artículo 8 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 8. Las solicitudes de asistencia jurídica podrán presentarse por escrito o por cualquier otro medio que deje constancia escrita, en condiciones que permitan a la autoridad central cerciorarse de su autenticad y transmisión segura.

Las autoridades centrales acordarán por escrito los canales seguros de transmisión y la forma de constatar la autenticidad.

Las autoridades centrales darán prioridad a los intercambios de solicitudes de asistencia jurídica, documentos adjuntos e información adicional entre las autoridades centrales por medios electrónicos.

En cualquier caso, previa solicitud y en cualquier momento se podrá solicitar la presentación de los documentos físicos en original o copia autenticada.

Artículo 24. El artículo 10 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 10. Las solicitudes de asistencia jurídica internacional y demás documentos que con ella se envíen se presentarán traducidos al español o en un idioma aceptado por la República de Panamá en un convenio bilateral o multilateral del que sea parte. Todos los documentos, registros, declaraciones y otros materiales en virtud de la

presente Ley están exentos de cualquier requisito de legalización, autenticación y otras formalidades.

Artículo 25. El artículo 13 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 13. La autoridad competente, sin solicitud previa, podrá comunicar a otro Estado información obtenida en el marco de sus propias investigaciones penales cuando considere que la revelación de dicha información podría ayudar a dicho Estado a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en su legislación interna, o podría dar lugar a una solicitud de cooperación de su parte.

Antes de comunicar dicha información, la autoridad competente podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones.

Artículo 26. Se adiciona el artículo 14 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 14. Se podrá denegar la asistencia si la solicitud se refiere a un delito que se considera delito político o delito vinculado a un delito político, o se considera que la ejecución de la solicitud podría atentar contra la soberanía, seguridad, orden público u otros intereses esenciales.

De igual forma, se podrá posponer la actuación en respuesta a una solicitud cuando pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por las autoridades.

En todo caso, antes de denegar o posponer la asistencia, se estudiará, previa consulta con el Estado requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que se consideren necesarias.

Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada.

También se informará al Estado requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

Artículo 27. Se adiciona el artículo 15 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 15: Cuando un Estado requirente solicite la conservación rápida de datos almacenados por medio de un sistema informático, el Ministerio Público podrá ordenarlo o asegurar los mismos de cualquier otra forma, de conformidad con las disposiciones establecidas en la legislación nacional.

Para los efectos del presente artículo, en las solicitudes de asistencia internacionales el Estado requirente indicará:

1. La autoridad que solicita dicha conservación;
2. El delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;
3. Los datos informáticos almacenados que deben conservarse y su relación con el delito;
4. Cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;
5. La necesidad de la conservación, y
6. Que el Estado requirente tiene la intención de presentar una solicitud de asistencia jurídica internacional para el registro o el acceso de forma similar, la incautación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

Cuando el Estado panameño considere que la conservación por sí sola no sea suficiente para garantizar la futura disponibilidad de los datos, o ponga en peligro la confidencialidad de la investigación del Estado requirente o pueda causar cualquier otro perjuicio a la misma, informará de ello sin demora al solicitante, para que decida si debe, pese a ello, procederse a la ejecución de la medida.

Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el presente artículo tendrán una duración mínima de sesenta días, sin perjuicio de que se pueda conceder una prórroga hasta la presentación de la solicitud de asistencia jurídica internacional.

Artículo 28. Se adiciona el artículo 16 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 16. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo anterior para la conservación de datos sobre el tráfico en relación con una comunicación específica, la autoridad competente descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación,

revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

Artículo 29. Se adiciona el artículo 17 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 17. Se prestará asistencia para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en el territorio transmitidas por medio de un sistema informático. Dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

De igual forma, se prestará la asistencia para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático, de conformidad con el derecho interno aplicable.

Artículo 30. Se adiciona el artículo 18 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 18. Se podrá diligenciar, una asistencia jurídica internacional con rapidez cuando se considere que existe una situación de emergencia, en la que exista un riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas.

Las solicitudes presentadas en virtud del presente artículo incluirán, además del contenido requerido, una descripción de los hechos que demuestren que existe una emergencia y cómo esta concierne a la asistencia solicitada.

Las peticiones en estos casos podrán ser transmitidas entre autoridades competentes, remitiéndose de forma simultánea una copia a la autoridad central del país requerido a través de la autoridad central del Estado requirente.

Las autoridades centrales acordarán por escrito los canales seguros de transmisión y la forma de constatar la autenticidad. Las autoridades competentes panameñas podrán solicitar con rapidez información complementaria para valorar la solicitud. De considerarse viable, se responderá oportunamente.

Previa solicitud del Estado requirente se podrán proporcionar los resultados de la ejecución de la solicitud o una copia, a través de un canal distinto del utilizado para la solicitud.

Para las situaciones de emergencia se garantizará que la autoridad central y la autoridad competente estén disponibles en todo momento habilitando los canales de comunicación correspondientes.

Artículo 31. Se adiciona el artículo 19 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 19. Se brindará asistencia para receptar el testimonio o declaraciones por videoconferencia o tecnología similar.

Las solicitudes de empleo de videoconferencia deben contener además de los requisitos establecidos en la presente Ley, el nombre y función de las autoridades del Estado requirente que participarán, las medidas relativas a la protección de la persona a ser oída, de ser necesario y cualquier aspecto relevante en relación a las condiciones para su ejecución.

La autoridad competente panameña y el Estado requirente procurarán facilitar la solución de cualquier problema que pueda surgir en relación con la ejecución de la solicitud de videoconferencia, de conformidad con la legislación interna del Estado requerido.

Las autoridades competentes procurarán que la persona cuyo testimonio o declaración se solicita comparezca en la fecha y horario acordado. La videoconferencia tendrá lugar en presencia de la autoridad competente panameña, se efectuará directamente por la autoridad competente del Estado requirente, o bajo su dirección, de conformidad con su legislación interna, y respetando los derechos y garantías previstos por ambos ordenamientos jurídicos.

Si la ejecución de la videoconferencia supone gastos de carácter extraordinario, se consultarán con el Estado requirente para determinar las condiciones en las que podrá ejecutarse la solicitud.

Artículo 32. Se adiciona el artículo 20 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 20. Las autoridades competentes podrán crear Equipos Conjuntos de Investigación en relación con investigaciones penales, que, por su complejidad investigativa, ameriten una coordinación de acciones con otras jurisdicciones, a fin de lograr resultados más efectivos en la investigación, pudiendo intercambiar de forma directa, la evidencia a partir de su conformación de conformidad con las siguientes previsiones:

1. Las solicitudes de creación de Equipos Conjuntos de Investigación, deberán contener:

a. Descripción de los motivos que ameritan la necesidad de su creación;
b. Descripción de los procedimientos de investigación que se propongan realizar;
c. Identificación de las autoridades competentes de la Parte Requirente para su integración;
d. Plazo estimado de duración del Equipo Conjunto de Investigación; y,
e. Los procedimientos que serán necesarios realizar, y
f. Cualquier otra información necesaria.

2. Una vez acordada la creación del Equipo Conjunto de Investigación, las autoridades competentes a cargo de las investigaciones elaborarán y firmarán el respectivo Instrumento de creación y funcionamiento, que deberá contener entre otros aspectos los fines específicos, la composición, las funciones, la duración y prórrogas, la ubicación, organización, requisitos aplicables a la recopilación, transmisión y utilización de información o pruebas, cláusulas de confidencialidad y condiciones para la participación de las autoridades en las actividades de investigación que tengan lugar en el territorio de otro de los países que lo integran, de conformidad con sus respectivas legislaciones internas.

3. Una vez concluidas las funciones del Equipo Conjunto de Investigación se deberá elaborar un Acta de Terminación.

Artículo 33. Se adiciona el artículo 21 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 21. Los datos personales transmitidos al Estado requirente en virtud de solicitudes de asistencia jurídica internacional, sólo podrán ser utilizados para los fines por los que fueron transmitidos y sujeto a las condiciones específicas debidamente motivadas establecidas por la autoridad que los transmitió. La utilización de los datos para otros fines por el Estado requirente necesita del consentimiento previo de la autoridad que los transmitió, teniendo en consideración la protección de los datos en su derecho interno.

Artículo 34. Se adiciona el artículo 22 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 22. En aquellos convenios o tratados internacionales en materia penal, en los que se establezcan redes permanentes para garantizar una asistencia inmediata, el punto de contacto será designado por el Procurador General de la Nación.

Artículo 35. La presente Ley modifica los artículos 184, 185, 290 y 291 del Código Penal; el artículo 112 del Código Procesal Penal; los artículos 4, 6, 7, 8, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21 y 22 de la Ley 11 de 31 de marzo de 2015; adiciona los artículos 166-A, 184-A, 226-A, 289-A, 290-A, 292-A al Código Penal; los artículos 314-A, 338-A, 338-B, 338-C y 338-D al Código Procesal Penal, así como también adiciona el Capítulo VI al Título I del Libro Tercero del Código Procesal Penal.

Artículo 36. Esta Ley entrará en vigencia a partir de su promulgación.

COMUNÍQUESE Y CÚMPLASE,

Propuesto a la consideración de la Asamblea Nacional, hoy ____ de septiembre de 2024, por el suscrito Javier E. Caraballo Salazar, Procurador General de la Nación, de conformidad con el literal c, numeral 1 del artículo 165 de la Constitución Política de la República.

Javier E. Caraballo Salazar
Procurador General de la Nación

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Trámite Legislativo
2024 - 2029

Código AN_SG_10
Versión 0
Fecha de versión 7-may-2024

		PERIODO LEGISLATIVO	2024 - 2025
Anteproyecto de Ley N°	23	Proyecto de Ley N°	45
Ley N°		Gaceta Oficial	
Etapa	PENDIENTE DE I DEBATE		

INFORMACIÓN GENERAL

Fecha de Presentación	08-jul-24	Comisión	GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES
Título	QUE ESTABLECE POLITICAS DE PREVENCION Y PROTECCION CONTRA LA VIOLENCIA SEXUAL DIGITAL Y MEDIATICA; ADICIONA DISPOSICIONES AL CÓDIGO PENAL Y DICTA OTRAS DISPOSICIONES.		
Proponente:	**HD Rodríguez Batista, Yarelis Anayansi**		
Coproponente:	HD Bloise Iglesias, Jorge Isaac	HD Cheng Peñalba, Manuel	
	HD Campos Lima, Miguel Ángel	HD Prado Castaño, Janine	
	HD Ulate Rodríguez, Lenín Alberto	HD González López, Jorge Alberto	
	HD Lee Rentería, Patsy Cristina	HD Gaitán Beitía, Eduardo Alejandro	
	HD Chong Smith, Yamireliz Daymirelkis	HD Duke Walker, Luis Henrique	
	HD Samaniego Rodríguez, Manuel Alberto	HD Brenes Samaniego, Alexandra María	
	HD Hernández Lacayo, Graciela Mercedes		

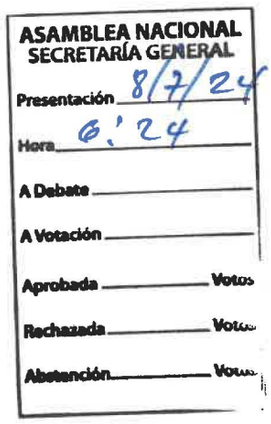
DEBATES

Fecha de Prohijamiento	27-ago-24
Fecha de I Debate	
Fecha de II Debate	
Fecha de III Debate	

Observaciones:	

ANTEPROYECTO DE LEY N°023
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

Panamá, 08 de julio de 2024



Honorable Diputada

DANA CASTAÑEDA

Presidenta de la Asamblea Nacional

E. S. D.

Señora Presidente:

Haciendo uso de la iniciativa legislativa que me confiere el artículo 108 del Reglamento Orgánico del Régimen Interno de la Asamblea Nacional y actuando en mi condición de Diputada de la República, presento al pleno de esta Asamblea Nacional el Anteproyecto de "**LEY QUE ESTABLECE POLÍTICAS DE DE PREVENCIÓN Y PROTECCIÓN CONTRA LA VIOLENCIA SEXUAL DIGITAL Y MEDIÁTICA; ADICIONA DISPOSICIONES AL CÓDIGO PENAL Y DICTA OTRAS DISPOSICIONES**", el cual merece exposición de motivos:

EXPOSICIÓN DE MOTIVOS

La evolución de las tecnologías de la información y la comunicación ha transformado profundamente la manera en que interactuamos, trabajamos y nos comunicamos. Sin embargo, junto con estas oportunidades, han surgido nuevos desafíos y amenazas que requieren una respuesta jurídica robusta y actualizada. En este contexto, el presente anteproyecto de ley tiene como objetivo proteger a todas las personas contra la violencia digital y mediática, estableciendo medidas preventivas, sanciones y herramientas de investigación moderna para combatir conductas que atenten contra la integridad, dignidad y derechos de las personas en el espacio digital y mediático.

Protección contra la Violencia Sexual Digital

Con el avance de la tecnología y las comunicaciones, han surgido nuevas formas de violencia que nuestras normas vigentes no pueden abordar adecuadamente. La violencia sexual digital es una de estas formas, y su impacto puede ser devastador. Es fundamental que nuestras leyes evolucionen

para proteger a las personas de abusos y vulneraciones en línea, salvaguardando tanto sus experiencias privadas como públicas. Esta modalidad de violencia incluye la difusión no consensuada de contenido íntimo, el uso de tecnologías de la información para humillar o extorsionar, y la creación de montajes pornográficos con la imagen de una persona. La falta de una definición clara y de medidas adecuadas para enfrentar esta forma de violencia agrava el problema, dejando a las víctimas desprotegidas y desamparadas.

Hace unos años, una figura pública conocida presentadora de TV, panameña, fue víctima de violencia sexual digital. Sus imágenes íntimas fueron divulgadas sin su consentimiento, afectando profundamente su vida personal y profesional. El caso de la presentadora de TV es un claro ejemplo de cómo la violencia sexual digital puede devastar la vida de una persona, resaltando la necesidad urgente de una legislación que proteja a los ciudadanos de estos abusos.

Beneficios del Anteproyecto de Ley

1. **Protección Integral de los Derechos Humanos**: Este anteproyecto de ley busca garantizar la protección integral de los derechos humanos en el entorno digital. Al establecer medidas preventivas y sanciones claras, se promueve un entorno digital más seguro y respetuoso, protegiendo la dignidad y privacidad de las personas.

   Derecho Comparado:

   - **España**: La Ley Orgánica 1/2004 de Medidas de Protección Integral contra la Violencia de Género incluye medidas contra la violencia digital.
   - **México**: La Ley Olimpia sanciona la difusión de contenido íntimo sin consentimiento.
   - **Argentina**: La Ley 26.904 incluye la violencia mediática y digital.

2. **Prevención y Educación**: La implementación de programas educativos y campañas de concienciación es una herramienta clave para prevenir la violencia digital. Estos programas no solo educarán a los jóvenes sobre el uso seguro de las tecnologías, sino que también capacitarán a padres y educadores para reconocer y actuar ante posibles casos de violencia digital.

Derecho Comparado:

- **España**: Incluye programas educativos sobre la violencia digital en su marco legal.
- **México**: Promueve programas de sensibilización y prevención en su legislación contra la violencia digital.

3. **Respuestas Adaptadas para Menores de Edad**: El anteproyecto dedica especial atención a la protección de los menores de edad, implementando medidas específicas para su protección y programas de educación adaptados a su edad y desarrollo. Esto asegura que los menores estén equipados con el conocimiento y las herramientas necesarias para navegar de manera segura en el entorno digital.

   Derecho Comparado:

   - **Colombia**: La Ley 1922 de 2018 aumenta las penas en casos de violencia digital contra menores.
   - **Perú**: El Decreto Legislativo 1410 incluye agravantes específicas para delitos de violencia sexual digital cuando las víctimas son menores.

4. **Utilización de Herramientas de Investigación Moderna**: La incorporación de tecnologías avanzadas como la inteligencia artificial y la cooperación internacional fortalece la capacidad de las autoridades para detectar y combatir la violencia digital de manera efectiva y en tiempo real.

   Derecho Comparado:

   - **España**: Utiliza herramientas tecnológicas avanzadas para la investigación de delitos digitales.
   - **México:** Ha implementado plataformas y mecanismos tecnológicos para denunciar y actuar rápidamente en casos de violencia digital.

MAC 13-1

MAC 9-1

5. **Sanciones Diferenciadas y Adaptadas**: La ley propone sanciones adecuadas para adultos y menores, buscando no solo castigar, sino también rehabilitar y educar a los infractores menores de edad. Esto promueve un enfoque más humano y eficaz en la administración de justicia.

Derecho Comparado:

- **Brasil**: La Ley 13.718 de 2018 establece sanciones y medidas de protección específicas para las víctimas de violencia digital.
- **Uruguay**: La Ley 19.580 ofrece apoyo legal y psicológico para las víctimas, además de sanciones adecuadas.

Iniciativas Internacionales y Derecho Comparado

La respuesta legislativa a la violencia digital ha ido evolucionando a lo largo de las últimas dos décadas, reflejando un creciente reconocimiento de la necesidad de protección en el entorno digital.

Evolución Cronológica de la Legislación Mundial en Materia de Violencia Digital:

1. **2001**: El Convenio de Budapest sobre Ciberdelincuencia marca un hito importante, estableciendo el primer tratado internacional que aborda los delitos informáticos y la evidencia electrónica, incluyendo delitos de contenido como la pornografía infantil y la violación de derechos de autor.
2. **2004**: España introduce la Ley Orgánica 1/2004 de Medidas de Protección Integral contra la Violencia de Género, que incluye medidas contra la violencia digital, reconociendo la creciente amenaza que representan las tecnologías de la información y comunicación en la perpetuación de la violencia de género.
3. **2008**: En los Estados Unidos, la Ley de Protección de Víctimas de la Pornografía Infantil enmienda el Código Penal para incluir disposiciones específicas contra la explotación y abuso infantil en el entorno digital.

MAC 13-1

MAC 9-1

4. **2013**: Nueva Zelanda adopta la Ley de Comunicaciones Digitales Dañinas, estableciendo un marco legal para abordar la difusión de contenido dañino en línea y proporcionando mecanismos de resolución rápida para las víctimas.
5. **2016**: Francia implementa la Ley para una República Digital, que incluye disposiciones contra el acoso en línea y la difusión no consentida de contenido íntimo.
6. **2018**: El Reino Unido actualiza su Ley de Protección de Datos con el Reglamento General de Protección de Datos (GDPR) de la UE, fortaleciendo las sanciones contra la violación de la privacidad y el manejo indebido de datos personales, incluidas las imágenes íntimas.
7. **2019**: México aprueba la Ley Olimpia, una serie de reformas legislativas a nivel federal y estatal que tipifican y sancionan la violencia digital, incluyendo la difusión de contenido íntimo sin consentimiento.
8. **2021**: Australia introduce la Ley de Seguridad Online, que establece nuevas regulaciones para proteger a los usuarios, especialmente menores, contra el ciberacoso, la explotación y otros daños en línea.

Cuadro Comparativo de Derecho Comparado en Latinoamérica:

País	**Legislación**	**Protección Legal**	**Aumento de Penas en Casos Agravados**	**Medidas de Protección para las Víctimas**	**Fuente**
México	Ley Olimpia (2019)	Sí	Sí, en casos de menores y relaciones de confianza	Sí	Diario Oficial de la Federación
Argentina	Ley 26.904	Sí	No	Sí	Boletín Oficial
Chile	Ley 21.153 (2018)	Sí	No	Sí	Biblioteca del Congreso Nacional de Chile
Colombia	Ley 1922 de 2018	Sí	Sí, en casos de menores	No	Congreso de la República de Colombia
Perú	Decreto Legislativo 1410	Sí	Sí, en casos de menores y relaciones de confianza	No	Diario Oficial El Peruano
Brasil	Ley 13.718 de 2018	Sí	No	Sí	Portal Planalto
Uruguay	Ley 19.580	Sí	No	Sí	Instituto Nacional de Estadística de Uruguay (INE)

MAC 9-1

Datos Estadísticos:

País	Casos Reportados de Violencia Sexual Digital (2023)	Población Total (2023)	Proporción de Casos por cada 100,000 Habitantes	Fuente
México	8,200	128,649,565	6.37	Instituto Nacional de Estadística y Geografía (INEGI)
Argentina	4,500	45,376,763	9.92	Instituto Nacional de Estadística y Censos (INDEC)
Chile	2,300	19,492,605	11.80	Instituto Nacional de Estadísticas (INE)
Colombia	5,100	51,265,844	9.95	Departamento Administrativo Nacional de Estadística (DANE)
Perú	3,800	33,684,208	11.28	Instituto Nacional de Estadística e Informática (INEI)
Brasil	15,000	214,326,223	7.00	Instituto Brasileiro de Geografia e Estatística (IBGE)
Uruguay	900	3,550,675	25.35	Instituto Nacional de Estadística de Uruguay (INE)

Basándonos en los datos del cuadro proporcionado sobre la violencia sexual digital en varios países de América Latina, podemos observar que Uruguay tiene la tasa más alta de casos reportados por cada 100,000 habitantes, con 25.35. Esta realidad subraya la urgencia de actualizar el marco legal para proteger a los ciudadanos contra la violencia sexual digital.

Impacto en el Seno Familiar y Consecuencias para la Sociedad

La violencia sexual digital tiene un impacto devastador en la confianza y la seguridad dentro de las familias. Las víctimas pueden experimentar un profundo estrés emocional, y la dinámica familiar puede verse afectada. A nivel social, las tasas elevadas de violencia sexual digital pueden contribuir a la normalización de comportamientos abusivos y coercitivos, requerir políticas más sólidas y medidas legislativas, y generar costos significativos para las víctimas y los sistemas de salud pública y servicios sociales.

MAC 13-C

MAC 9-1

Por lo antes mencionado, se somete a la consideración de la Asamblea Nacional el Anteproyecto de "LEY QUE ESTABLECE POLÍTICAS DE PREVENCIÓN Y PROTECCIÓN CONTRA LA VIOLENCIA SEXUAL DIGITAL Y MEDIÁTICA; ADICIONA DISPOSICIONES AL CÓDIGO PENAL Y DICTA OTRAS DISPOSICIONES". Esta ley no solo llenará un vacío legal existente, sino que también proporcionará un marco claro y específico para la protección de los derechos de las personas en el entorno digital, promoviendo un entorno seguro y respetuoso para todos los ciudadanos.

13-1

9-1

8-2

YARELIS RODRIGUEZ
Diputada de la República
Circuito 8-2

8-4

13-1

8-4

8-6

8-5

8-2

8-4
JORGE BLAKE

13-4

ANTEPROYECTO DE LEY No.

(____ de _____ de 2024)

"LEY QUE ESTABLECE POLÍTICAS DE PREVENCIÓN Y PROTECCIÓN CONTRA LA VIOLENCIA SEXUAL DIGITAL Y MEDIÁTICA; ADICIONA DISPOSICIONES AL CÓDIGO PENAL Y DICTA OTRAS DISPOSICIONES"

LA ASAMBLEA NACIONAL

DECRETA:

TITULO 1

DISPOSICIONES GENERALES

Artículo 1. Esta ley tiene como objeto proteger a todas las personas contra la violencia sexual digital y mediática, estableciendo medidas preventivas, sanciones y herramientas de investigación moderna para combatir conductas que atenten contra su integridad, dignidad y derechos en el espacio digital y mediático.

Artículo 2. Esta Ley es de interés social. Todas las medidas que se deriven de ella garantizarán la prevención, atención, sanción erradicación de cualquier tipo de Violencia Sexual Digital y promoverán su desarrollo integral y plena participación en todas las esferas.

Artículo 3. Esta Ley se aplicará cuando las conductas descritas en ella se dirijan contra mujeres, hombres o menores de edad, debido a la vulnerabilidad que implica la exposición a las nuevas tecnologías de la información. En este contexto, se entenderán las siguientes conductas: Violencia Sexual Digital, Violencia Mediática, uso de Tecnologías de la Información y la Comunicación, sexting y ciberacoso.

La Ley debe interpretarse según los principios contenidos en la Constitución Política de la República, las leyes y los tratados o convenios internacionales de derechos humanos notificados por la República de Panamá e igualmente el convenio de Budapest sobre Ciberdelincuencia.

J.M.G.C 9-5 MAC 9-1 9-1

Artículo 4. Se entenderá como Violencia Sexual Digital toda conducta, acción u omisión en contra de las mujeres, hombres y menores de edad que sea cometida, instigado o agravada, en parte o en su totalidad, con la asistencia, utilización y/o apropiación de las tecnologías de la información y la comunicación, con el objeto de causar daños físicos, psicológicos, económicos, sexuales o morales tanto en el ámbito privado como en el público o su grupo familiar.

TITULO II

DEFINICIONES Y PRINCIPIOS

Artículo 5. Para los efectos de esta ley, se entiende por:

- **Violencia Sexual Digital:** Toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, que exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, causando daño psicológico, emocional, en su vida privada o en su imagen propia. Esto incluye, pero no se limita a, la distribución no consentida de material íntimo, conocido comúnmente como "revenge porn" o "nudes packs".
- **Violencia Mediática:** Todo acto a través de cualquier medio de comunicación, que de manera directa o indirecta promueva estereotipos sexistas, haga apología de la violencia contra las personas, produzca o permita la producción y difusión de discurso de odio sexista, discriminación de género o desigualdad entre géneros, causando daño psicológico, sexual, físico, económico, patrimonial o en extremo, feminicida o misándrico.
- **Tecnologías de la Información y la Comunicación:** Recursos, herramientas y programas utilizados para procesar, administrar y compartir información mediante diversos soportes tecnológicos. Esto incluye dispositivos digitales, software, internet, redes sociales y plataformas de comunicación.
- **Sexting:** El envío de mensajes, fotos o videos de contenido sexual explícito, principalmente a través de dispositivos móviles. Esta práctica sin el consentimiento adecuado se considera una forma de violencia digital cuando se utiliza para acosar, amenazar o exponer públicamente a alguien.

MAC MC

- **Ciberacoso:** El uso de las tecnologías de la información para acosar, intimidar o agredir a una persona de manera repetida y deliberada. Incluye, pero no se limita a, acoso en redes sociales, correos electrónicos amenazantes o difamatorios, y el uso malintencionado de datos personales.

TITULO III

MODALIDADES DE LA VIOLENCIA

CAPÍTULO I: De la Violencia Sexual Digital y Mediática

Artículo 6. La violencia sexual digital y mediática será sancionada conforme a las disposiciones del Código Penal de la República de Panamá.

CAPÍTULO II: Violencia Sexual Digital y Mediática contra Menores

Artículo 7. Específicamente se enfocará en proteger a los menores de edad, implementando medidas de protección adicionales y programas de educación y sensibilización adaptados a su edad y desarrollo.

- **Medidas de Protección Específicas:** Creación de un protocolo de acción rápida para casos donde menores estén involucrados, asegurando una respuesta inmediata y adecuada por parte de las autoridades.
- **Programas Educativos:** Integración de módulos específicos sobre seguridad en línea y el impacto de la violencia digital en la vida de los jóvenes, en los currículos escolares.

TÍTULO IV

MEDIDAS PREVENTIVAS Y HERRAMIENTAS DE INVESTIGACIÓN

Artículo 8. Medidas Preventivas. Las autoridades competentes deberán implementar medidas preventivas ampliadas:

- **Campañas Educativas:** Enfocadas también en padres y educadores, proporcionando herramientas para reconocer y actuar frente a la violencia sexual digital y mediática.

MAC 9-1

9-1

- **Fomento de Aplicaciones Seguras:** Promoción de tecnologías y aplicaciones que incorporen medidas de seguridad avanzadas para proteger a los usuarios contra la violencia digital.

El Ministerio de Educación creará programas de alfabetización digital, buenas prácticas en el uso de las tecnologías de la información y la comunicación, así como también, de identificación de las violencias sexual digitales, en las clases de educación sexual integral como en el resto de los contenidos en el ámbito educativo y en la formación docente.

Artículo 9. Herramientas de Investigación Moderna. Además de las herramientas ya mencionadas, se incorporarán:

- **Inteligencia Artificial:** Utilización de IA para detectar y alertar sobre posibles casos de violencia digital en tiempo real.
- **Cooperación Internacional:** Establecimiento de mecanismos de cooperación internacional para la persecución de delitos que trascienden fronteras nacionales.
- **Auditorías Digitales:** Implementación de auditorías periódicas a empresas que gestionan plataformas digitales, para asegurar el cumplimiento de normativas de protección a la infancia y la mujer.

En la investigación la autoridad interviniente ordenará al presunto agresor que cese en los actos de perturbación o intimidación que, directa o indirectamente, tanto en el espacio analógico como en el digital. Ordenará la prohibición de contacto del presunto agresor hacia la víctima que padece violencia sexual por intermedio de cualquier tecnología de la información y la comunicación, aplicación de mensajería instantánea o canal de comunicación digital.

La autoridad interviniente ordenará a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, de manera escrita o electrónica la supresión de contenidos que constituyan un ejercicio de la violencia digital o telemática definida en la presente ley, debiendo identificarse en la orden la URL específica del contenido cuya remoción se ordena.

MAC
9-1

9-1

TÍTULO V

ASIGNACIONES PRESUPUESTARIAS

Artículo 10. Los recursos para llevar a cabo los programas y la implementación de las acciones que se deriven en la ley se cubrirá con el presupuesto autorizado a las entidades e instituciones autónomas del Estado.

1. Creación de una comisión interinstitucional encargada de promover, vigilar y dar seguimiento a los programas señalados en la ley.
2. Fortalecimiento al Instituto de Medicina Legal y Ciencias Forenses, con los recursos y herramientas para hacer frente a los nuevos desafíos que se encuentra en materia de tecnologías.
3. Fortalecimiento la Secretaría de la Niñez y Adolescencia, a fin de promover medidas de prevención contra la Violencia Sexual Digital en bienestar de los menores de edad.
4. Fortalecimiento al Ministerio de Educación a fin de poder promover políticas educativas sobre los nuevos desafíos digitales a los que pueden encontrarse los menores de edad en la etapa primaria, secundaria y universitaria.

TÍTULO VI

DISPOSICIONES FINALES

Artículo 11. Actualización y Revisión de la Ley. La ley será revisada y actualizada cada dos años para adaptarse a los avances tecnológicos y las nuevas modalidades de violencia sexual digital y mediática.

Artículo 12. Se adiciona el artículo 178 A al Código Penal, así:

Artículo 178 A. Quien difunda mediante el uso de tecnologías de la información y la comunicación (TIC) contenido íntimo sexual o de desnudez en donde se exponga, distribuya, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, impresiones gráficas, audios o videos, reales o simulados, de una persona sin su consentimiento, sin su aprobación o sin su autorización

MAC 9-1 9-1

y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia, será sancionado de tres a seis años de prisión.

La pena será aumentada hasta un tercio:

1) Si el hecho se cometiere por la persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aún sin convivencia.

2) Si el hecho se cometiere con fin de lucro.

3) Si el hecho se cometiere por placer, codicia, odio racial, religioso o político.

4) Si el hecho se cometiere contra un (a) menor de edad.

5) Si el hecho es utilizado por medio de cuentas falsas para esconder su verdadera identidad.

6) Si el hecho la víctima tuviera algún grado de incapacidad o se encontrara en estado de inconsciencia.

Artículo 13. Reglamentación. El Órgano Ejecutivo reglamentará la presente ley dentro de seis meses desde su entrada en vigencia.

Esta redacción ampliada aborda de manera integral la protección contra la violencia sexual digital, con un enfoque especial en los menores de edad y adaptando las sanciones para ser apropiadas y educativas cuando corresponda.

Artículo 14. La presente ley adiciona el artículo 178 A al Código Penal.

Artículo 15. Promulgación. Esta ley comenzara a regir a los seis meses de su promulgación.

COMUNÍQUESE Y CÚMPLASE

Propuesto a la consideración de la Asamblea Nacional el día de hoy ___ de _____ de 2024, por la Honorable Diputada **YARELIS RODRIGUEZ.**

YARELIS RODRIGUEZ

Diputada de la República

Circuito 8-2

PROYECTO DE LEY Nº0045
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Presentación 22/8/24
Hora 5:44

Comisión de Gobierno, Justicia y Asuntos Constitucionales

H.D. Luis E. Camacho
Presidente

Tel. (507) 512-8083
Fax. (507) 512-8120

Panamá, 27 de AGOSTO de 2024.
2024_086_AN_CGJYAC.

Honorable Diputada
DANA CASTAÑEDA GUARDIA
Presidente de la Asamblea Nacional
Presente

Señora Presidente:

En cumplimiento del artículo 109 del Reglamento Orgánico del Régimen Interno de la Asamblea Nacional, debidamente analizado y prohijado por esta Comisión en su sesión del día 27 de agosto de 2024, remitimos el Proyecto de Ley **"Que establece políticas de prevención y protección contra la violencia sexual digital y mediática; adiciona disposiciones al Código Penal y dicta otras disposiciones"**, que corresponde al Anteproyecto de Ley N° 23, originalmente presentado por la Honorable Diputada Yarelis Rodríguez.

Le solicitamos se sirva impartir el trámite de rigor, con el objeto que la citada iniciativa legislativa sea sometida próximamente al primer debate.

Atentamente,

Luis Eduardo Camacho Castro
Presidente

LEC/dv

EXPOSICIÓN DE MOTIVOS

La evolución de las tecnologías de la información y la comunicación ha transformado profundamente la manera en que interactuamos, trabajamos y nos comunicarnos. Sin embargo, junto con estas oportunidades, han surgido nuevos desafio s y amenazas que requieren una respuesta jurídica robusta y actualizada. En este contexto, el presente anteproyecto de ley tiene corno objetivo proteger a todas las personas contra la violencia digital y mediática, estableciendo medidas preventivas, sanciones y herramientas de investigación moderna para combatir conductas que atenten contra la integridad, dignidad y derechos de las personas en el espacio digital y mediático.

Protección contra la Violencia Sexual Digital

Con el avance de la tecnología y las comunicaciones, han surgido nuevas formas de violencia que nuestras normas vigentes no pueden abordar adecuadamente. La violencia sexual digital es una de estas formas, y su impacto puede ser devastador. Es fundamental que nuestras leyes evolucionen para proteger a las personas de abusos y vulneraciones en línea, salvaguardando tanto sus experiencias privadas como públicas. Esta modalidad de violencia incluye la difusión no consensuada de contenido íntimo, el uso de tecnologías de la información para humillar o extorsionar, y la creación de montajes pornográficos con la imagen de una persona. La falta de una definición clara y de medidas adecuadas para enfrentar esta forma de violencia agrava el problema, dejando a las víctimas desprotegidas y desamparadas.

Hace unos años, una figura pública conocida presentadora de TV, panameña, fue víctima de violencia sexual digital. Sus imágenes íntimas fueron divulgadas sin su consentimiento, afectando profundamente su vida personal y profesional. El caso de la presentadora de TV es un claro ejemplo de cómo la violencia sexual digital puede devastar la vida de una persona, resaltando la necesidad urgente de una legislación que proteja a los ciudadanos de estos abusos.

Beneficios del Anteproyecto de Ley

1. **Protección Integral de los Derechos Humanos:** Este anteproyecto de ley busca garantizar la protección integral de los derechos humanos en el entorno digital. Al establecer medidas preventivas y sanciones claras, se promueve un entorno digital más seguro y respetuoso, protegiendo la dignidad y privacidad de las personas.

Derecho Comparado:

- **España:** La Ley Orgánica 1/2004 de Medidas de Protección Integral contra la Violencia de Género incluye medidas contra la violencia digital.
- **México:** La Ley Olimpia sanciona la difusión de contenido íntimo sm consentimiento.
- **Argentina:** La Ley 26.904 incluye la violencia mediática y digital.

Derecho Comparado:

- **Brasil:** La Ley 13.718 de 2018 establece sanciones y medidas de protección específicas para las víctimas de violencia digital.
- **Uruguay:** La Ley 19.580 ofrece apoyo legal y psicológico para las víctimas, además de sanciones adecuadas.

Iniciativas Internacionales y Derecho Comparado

La respuesta legislativa a la violencia digital ha ido evolucionando a 10 largo de las últimas dos décadas, reflejando un creciente reconocimiento de la necesidad de protección en el entorno digital.

Evolución Cronológica de la Legislación Mundial en Materia de Violencia Digital:

1. **2001:** El Convenio de Budapest sobre Ciberdelincuencia marca un hito importante, estableciendo el primer tratado internacional que aborda los delitos informáticos y la evidencia electrónica, incluyendo delitos de contenido como la pomografla infantil y la violación de derechos de autor.
2. **2004:** España introduce la Ley Orgánica 1/2004 de Medidas de Protección Integral contra la Violencia de Género, que incluye medidas contra la violencia digital, reconociendo la creciente amenaza que representan las tecnologías de la información y comunicación en la perpetuación de la violencia de género.
3. **2008:** En los Estados Unidos, la Ley de Protección de Víctimas de la Pomografla Infantil enmienda el Código Penal para incluir disposiciones específicas contra la explotación y abuso infantil en el entorno digital
4. **2013:** Nueva Zelanda adopta la Ley de Comunicaciones Digitales Dañinas, estableciendo un marco legal para abordar la difusión de contenido dañino en línea y proporcionando mecanismos de resolución rápida para las víctimas.
5. **2016:** Francia implementa la Ley para una República Digital, que incluye disposiciones contra el acoso en línea y la difusión no consentida de contenido íntimo.
6. **2018:** El Reino Unido actualiza su Ley de Protección de Datos con el Reglamento General de Protección de Datos (GDPR) de la UE, fortaleciendo las sanciones contra la violación de la privacidad y el manejo indebido de datos personales, incluidas las imágenes íntimas.
7. **2019:** México aprueba la Ley Olimpia, una serie de reformas legislativas a nivel federal y estatal que tipifican y sancionan la violencia digital, incluyendo la difusión de contenido íntimo sin consentimiento.
8. **2021:** Australia introduce la Ley de Seguridad Online, que establece nuevas regulaciones para proteger a los usuarios, especialmente menores, contra el ciberacoso, la explotación y otros daños en línea.

Cuadro Comparativo de Derecho Comparado en Latinoamérica:

País	Legislación	Protección Legal	Aumento de Penas en Casos Agraavados	Medidas de Protección para las Victimas	Fuentes
México	Ley Olimpia (2019)	Si	Si, en casos de menores y relaciones de confianza	Si	Diario Oficial de la Federación
Argentina	Ley 26.904	Si	No	Si	Boletín Oficial
Chile	Ley 21.153 (2018)	Si	No	Si	Biblioteca del Congreso Nacional de Chile
Colombia	Ley 1922 de 2018	Si	Si, en casos de menores	No	Congreso de la Republica de Colombia
Perú	Decreto Legislativo 1410	Si	Si, en casos de menores y relaciones de confianza	No	Diario Oficial El Peruano
Brasil	Ley 13.718 de 2018	Si	No	Si	Portal Planalto
Uruguay	Ley 19.580	Si	No	Si	Instituto Nacional de Estadística de Uruguay (INE)

Datos Estadísticos:

País	Casos Reportados de Violencia Sexual Digital (2023)	Población Total (2023)	Proporción de Casos por cada 100,000 Habitantes	Fuentes
México	8,200	128,649,565	6.37	Instituto Nacional de Estadística y Geografía (INEGI)
Argentina	4,500	45,376,763	9.92	Instituto Nacional de Estadística y Censos (INDEC)
Chile	2,300	19,492,605	11.80	Instituto Nacional de Estadística (INE)
Colombia	5,100	51,265,844	9.95	Departamento Administrativo Nacional de Estadística (DANE)
Perú	3,800	33,684,208	11.28	Instituto Nacional de Estadística e Informática (INEI)
Brasil	15,000	214,326,223	7.00	Instituto Brasileiro de Geografía e Estadística (IBGE)
Uruguay	900	3,550,675	25.35	Instituto Nacional de Estadística de Uruguay (INE)

Basándonos en los datos del cuadro proporcionado sobre la violencia sexual digital en varios países de América Latina, podemos observar que Uruguay tiene la tasa más alta de casos reportados por cada 100,000 habitantes, con 25.35. Esta realidad subraya la urgencia de actualizar el marco legal para proteger a los ciudadanos contra la violencia sexual digital.

Impacto en el Seno Familiar y Consecuencias para la Sociedad

La violencia sexual digital tiene un impacto devastador en la confianza y la seguridad dentro de las familias. Las víctimas pueden experimentar un profundo estrés emocional, y la dinámica familiar puede verse afectada. A nivel social, las tasas elevadas de violencia sexual digital pueden contribuir a la normalización de comportamientos abusivos y coercitivos, requerir políticas más sólidas y medidas legislativas, y generar costos significativos para las víctimas y los sistemas de salud pública y servicios sociales.

Por lo antes mencionado, se somete a la consideración de la Asamblea Nacional el Anteproyecto de "LEY QUE ESTABLECE POLÍTICAS DE PREVENCIÓN Y PROTECCIÓN CONTRA LA VIOLENCIA SEXUAL DIGITAL Y MEDIÁTICA; ADICIONA DISPOSICIONES AL CÓDIGO PENAL Y DICTA OTRAS DISPOSICIONES". Esta ley no solo llenará un vacío legal existente, sino que también proporcionará un marco claro y específico para la protección de los derechos de las personas en el entorno digital, promoviendo un entorno seguro y respetuoso para todos los ciudadanos.

PROYECTO DE LEY No._____

"QUE ESTABLECE POLÍTICAS DE PREVENCIÓN Y PROTECCIÓN CONTRA LA VIOLENCIA SEXUAL DIGITAL Y MEDIÁTICA; ADICIONA DISPOSICIONES AL CÓDIGO PENAL Y DICTA OTRAS DISPOSICIONES"

LA ASAMBLEA NACIONAL

DECRETA:

TITULO 1

DISPOSICIONES GENERALES

Artículo 1. Esta ley tiene como objeto proteger a todas las personas contra la violencia sexual digital y mediática, estableciendo medidas preventivas, sanciones y herramientas de investigación moderna para combatir conductas que atenten contra su integridad, dignidad y derechos en el espacio digital y mediático.

Artículo 2. Esta Leyes de interés social. Todas las medidas que se deriven de ella garantizarán la prevención, atención, sanción erradicación de cualquier tipo de Violencia Sexual Digital y promoverán su desarrollo integral y plena participación en todas las esferas.

Artículo 3. Esta Ley se aplicará cuando las conductas descritas en ella se dirijan contra mujeres, hombres o menores de edad, debido a la vulnerabilidad que implica la exposición a las nuevas tecnologías de la información. En este contexto, se entenderán las siguientes conductas: Violencia Sexual Digital, Violencia Mediática, uso de Tecnologías de la Información y la Comunicación, sexting y ciberacoso.

La Ley debe interpretarse según los principios contenidos en la Constitución Política de la República, las leyes y los tratados o convenios internacionales de derechos humanos notificados por la República de Panamá e igualmente el convenio de Budapest sobre Ciberdelincuencia.

Artículo 4. Se entenderá como Violencia Sexual Digital toda conducta, acción u omisión en contra de las mujeres, hombres y menores de edad que sea cometida, instigado o agravada, en parte o en su totalidad, con la asistencia, utilización y/o apropiación de las tecnologías de la información y la comunicación, con el objeto de causar daños físicos, psicológicos, económicos, sexuales o morales tanto en el ámbito privado como en el público o su grupo familiar.

TITULO 11

DEFINICIONES Y PRINCIPIOS

Artículo 5. Para los efectos de esta ley, se entiende por:

- **Violencia Sexual Digital:** Toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, que exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, causando daño psicológico, emocional, en su vida privada o en su imagen propia. Esto incluye, pero no se limita a, la distribución no consentida de material íntimo, conocido comúnmente como "revenge pom" o "nudes packs".
- **Violencia Mediática:** Todo acto a través de cualquier medio de comunicación, que de manera directa o indirecta promueva estereotipos sexistas, haga apología de la violencia contra las personas, produzca o permita la producción y difusión de discurso de odio sexista, discriminación de género o desigualdad entre géneros, causando daño psicológico, sexual, físico, económico, patrimonial o en extremo, feminicida o misándrico.
- **Tecnologías de la Información y la Comunicación:** Recursos, herramientas y programas utilizados para procesar, administrar y compartir información mediante diversos soportes tecnológicos. Esto incluye dispositivos digitales, software, intemet, redes sociales y plataformas de comunicación.
- **Sexting:** El envío de mensajes, fotos o videos de contenido sexual explícito, principalmente a través de dispositivos móviles. Esta práctica sin el consentimiento adecuado se considera una forma de violencia digital cuando se utiliza para acosar, amenazar o exponer públicamente a alguien.
- **Ciberacoso:** El uso de las tecnologías de la información para acosar, intimidar o agredir a una persona de manera repetida y deliberada. Incluye, pero no se limita a, acoso en redes sociales, correos electrónicos amenazantes o difamatorios, y el uso malintencionado de datos personales.

TITULO 111

MODALIDADES DE LA VIOLENCIA

CAPÍTULO 1: De la Violencia Sexual Digital y Mediática

Artículo 6. La violencia sexual digital y mediática será sancionada conforme a las disposiciones del Código Penal de la República de Panamá.

CAPÍTULO 11: Violencia Sexual Digital y Mediática contra Menores

Artículo 7. Específicamente se enfocará en proteger a los menores de edad, implementando medidas de protección adicionales y programas de educación y sensibilización adaptados a su edad y desarrollo.

• **Medidas de Protección Específicas:** Creación de un protocolo de acción rápida para casos donde menores estén involucrados, asegurando una respuesta inmediata y adecuada por parte de las autoridades.

• **Programas Educativos:** Integración de módulos específicos sobre seguridad en línea y el impacto de la violencia digital en la vida de los jóvenes, en los currículos escolares.

TÍTULO IV

MEDIDAS PREVENTIVAS Y HERRAMIENTAS DE INVESTIGACIÓN

Artículo 8. Medidas Preventivas. Las autoridades competentes deberán implementar medidas preventivas ampliadas:

• **Campañas Educativas:** Enfocadas también en padres y educadores, propñt/ando herramientas para reconocer y actuar frente a la violencia sexual digital y mediática.

• **Fomento de Aplicaciones Seguras:** Promoción de tecnologías y aplicaciones que incorporen medidas de seguridad avanzadas para proteger a los usuarios contra la violencia digital.

El Ministerio de Educación creará programas de alfabetización digital, buenas prácticas en el uso de las tecnologías de la información y la comunicación, así como también, de identificación de las violencias sexual digitales, en las clases de educación sexual integral como en el resto de los contenidos en el ámbito educativo y en la formación docente.

Artículo 9. Herramientas de Investigación Moderna. Además de las herramientas ya mencionadas, se incorporarán:

• **Inteligencia Artificial:** Utilización de lA para detectar y alertar sobre posibles casos de violencia digital en tiempo real.

• **Cooperación Internacional:** Establecimiento de mecamsmos de cooperación internacional para la persecución de delitos que trascienden fronteras nacionales.

• **Auditorías Digitales:** Implementación de auditorías periódicas a empresas que gestionan plataformas digitales, para asegurar el cumplimiento de normativas de protección a la infancia y la mujer.

En la investigación la autoridad interviniente ordenará al presunto agresor que cese en los actos de perturbación o intimidación que, directa o indirectamente, tanto en el espacio analógico como en el digital. Ordenará la prohibición de contacto del presunto agresor hacia la víctima que padece violencia sexual por intermedio de cualquier tecnología de la información y la comunicación, aplicación de mensajería instantánea o canal de comunicación digital.

La autoridad interviniente ordenará a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, de manera escrita o electrónica la supresión de contenidos que

constituyan un ejercicio de la violencia digital o telemática definida en la presente ley, debiendo identificarse en la orden la URL específica del contenido cuya remoción se ordena.

TÍTULO V

ASIGNACIONES PRESUPUESTARIAS

Artículo 10. Los recursos para llevar a cabo los programas y la implementación de las acciones que se deriven en la ley se cubrirá con el presupuesto autorizado a las entidades e instituciones autónomas del Estado.

1. Creación de una comisión interinstitucional encargada de promover, vigilar y dar seguimiento a los programas señalados en la ley.
2. Fortalecimiento al Instituto de Medicina Legal y Ciencias Forenses, con los recursos y herramientas para hacer frente a los nuevos desafíos que se encuentra en materia de tecnologías.
3. Fortalecimiento la Secretaría de la Niñez y Adolescencia, a fin de promover medidas de prevención contra la Violencia Sexual Digital en bienestar de los menores de edad.
4. Fortalecimiento al Ministerio de Educación a fin de poder promover políticas educativas sobre los nuevos desafíos digitales a los que pueden encontrarse los menores de edad en la etapa primaria, secundaria y universitaria.

TÍTULO VI

DISPOSICIONES FINALES

Artículo 11. Actualización y Revisión de la Ley. La ley será revisada y actualizada cada dos años para adaptarse a los avances tecnológicos y las nuevas modalidades de violencia sexual digital y mediática.

Artículo 12. Se adiciona el artículo 178 A al Código Penal, así: Artículo 178 A. Quien difunda mediante el uso de tecnologías de la información y la comunicación (TIC) contenido íntimo sexual o de desnudez en donde se exponga, distribuya, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, impresiones gráficas, audio s o videos, reales o simulados, de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia, será sancionado de tres a seis años de prisión.

La pena será aumentada hasta un tercio:

1) Si el hecho se cometiere por la persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aún sin convivencia.

2) Si el hecho se cometiere con fin de lucro.

3) Si el hecho se cometiere por placer, codicia, odio racial, religioso o político.

4) Si el hecho se cometiere contra un (a) menor de edad.

5) Si el hecho es utilizado por medio de cuentas falsas para esconder su verdadera identidad.
6) Si el hecho la víctima tuviera algún grado de incapacidad o se encontrara en estado de inconsciencia.

Artículo 13. Reglamentación. El Órgano Ejecutivo reglamentará la presente ley dentro de seis meses desde su entrada en vigencia.

Esta redacción ampliada aborda de manera integral la protección contra la violencia sexual digital, con un enfoque especial en los menores de edad y adaptando las sanciones para ser apropiadas y educativas cuando corresponda.

Artículo 14. La presente ley adiciona el artículo 178 A al Código Penal.

Artículo 15. Promulgación. Esta ley comenzara a regir a los seis meses de su promulgación.

COMUNÍQUESE Y CÚMPLASE.

Propuesto a la consideración del Pleno de la Asamblea Nacional, hoy 27 de agosto de 2024, por la Comisión de Gobierno, Justicia y Asuntos Constitucionales.

POR LA COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES

H.D. LUIS EDUARDO CAMACHO CASTRO
Presidente

H.D. ARIEL VALLARINO
Vicepresidente

H.D. FRANCISCO BREA
Secretario

H.D. CRISPIANO ADAMES NAVARRO
Comisionado

H.D. MANUEL CHENG
Comisionado

H.D. JOSÉ PÉREZ
Comisionado

H.D. RAÚL PINEDA
Comisionado

H.D. DIDIANO PINILLA
Comisionado

H.D. ROBERTO ZÚÑIGA
Comisionado

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Trámite Legislativo
2024 - 2029

Código AN_SG_10
Versión 0
Fecha de versión 7-may-2024

		PERIODO LEGISLATIVO	2024 - 2025
Anteproyecto de Ley N°	87	Proyecto de Ley N°	50
Ley N°		Gaceta Oficial	
Etapa	PENDIENTE DE I DEBATE		

INFORMACIÓN GENERAL

Fecha de Presentación	31-jul-24	Comisión	GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES
Título	QUE MODIFICA Y ADICIONA ARTICULOS AL CODIGO PENAL SOBRE DELITOS INFORMATICOS.		
Proponente:	**HD Coba Martínez, Ariana Marisin**		
Coproponente:	HD Campos Lima, Miguel Ángel	HD Rodríguez Batista, Yarelis Anayansi	
	HD Ulate Rodríguez, Lenín Alberto	HD Chong Smith, Yamireliz Daymirelkis	
	HD Prado Castaño, Janine		
	HD Duke Walker, Luis Henrique		
	HD Vega, Jhonathan Edir		
	HD Gaitán Beitía, Eduardo Alejandro		

DEBATES

Fecha de Prohijamiento	27-ago-24
Fecha de I Debate	
Fecha de II Debate	
Fecha de III Debate	

Observaciones:	

ANTEPROYECTO DE LEY N°087
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

Panamá, 29 de julio de 2024

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Presentación 31/7/24
Hora 6:13
A Debate
A Votación
Aprobada ____ Votos
Rechazada ____ Votos
Abstención ____ Votos

Honorable Diputada
DANA CASTAÑEDA GUARDIA
Presidente
Asamblea Nacional

Señora Presidente:

En ejercicio de la iniciativa legislativa que me confiere nuestra Carta Magna y el artículo 108 de nuestro Reglamento Orgánico del Régimen Interno, presento a la consideración de la Asamblea Nacional, el Anteproyecto de Ley, **Que modifica y adiciona artículos al Código Penal sobre Delitos Informáticos,** que merece la siguiente:

EXPOSICION DE MOTIVOS

Con el desarrollo de la internet se han roto barreras y se ha agilizado la comunicación en el mundo entero, dando paso a un sinnúmero de posibilidades para cada individuo al tener acceso a tanta información.

Esta disponibilidad se percibe en el gran número de usuarios de computadoras y otros dispositivos electrónicos existentes, que va en incremento al utilizarse no solo como un medio de comunicación sino para realizar compras, pagos, para la enseñanza, la atención médica, entre algunos usos o aplicaciones que se le pueda dar.

Vemos que por el tipo y calidad de la información que se trasmite a través de la red, que incluye imágenes e información personal o comercial, en muchos casos confidencial, se ha despertado el interés de los denominados delincuentes cibernéticos, que no solo atacan los sistemas informáticos, sino que han ampliado su rango de acción, cometiendo delitos como el fraude, la extorsión, la divulgación de información e imágenes sin autorización de la persona, amparados por incontables enlaces que les permiten actuar en el anonimato del mundo virtual o por darse la comisión en países donde no existe legislación sobre la materia o es muy escaza.

La escalada de los delitos informáticos en el mundo ha llevado a los países a desarrollar normativas para su prevención y sanción, corriente de la cual no escapa nuestro país.

Muchas son las denuncias que en los últimos años ha recibido el Ministerio Público, en especial las relacionadas con ataques a los sistemas informáticos, los de orden financiero, el acoso, hostigamiento y extorsión derivados de la violación de la privacidad y la violencia mediática, entre otros.

En ese sentido, en los últimos días se ha dado a conocer en las redes y medios de comunicación la comisión un delito informático de violación de la privacidad, que ha suscitado la repulsa de la sociedad y dejado claro, la necesidad de legislar sobre esta materia de manera más extensa para que la autoridad competente cuente con las herramientas para sancionar estos delitos, debido a que algunos de estos actos delictivos no se encuentran entre los tipos penales contenidos en el Código Penal vigente.

Atendiendo esa necesidad, presentamos esta iniciativa legislativa que contempla la modificación y adición de artículos al Código Penal vigente relativos a los delitos informáticos que desarrolla la extorsión, el acoso sexual, la violencia mediática y amplia los tipos penales de los artículos 289 al 292, que desarrollan delitos contra la seguridad informática, todo con la finalidad de contrarrestar los riesgos que estos generan para la sociedad, las empresas y los gobiernos.

También se hizo una revisión de las sanciones, aumentándose los años de prisión en algunos delitos, estableciendo las agravantes e incluyendo la inhabilitación para ejercer cargos públicos por el mismo tiempo de prisión.

Hacemos hincapié en los temas de violación de la intimidad de la persona y extorsión, porque es usual que quien se vea afectado por este tipo de violación, luego es forzado a dar, entregar o hacer algo para evitar que sus archivos sean trasmitidos por la red, para evitar así lo que se denomina violencia mediática.

Aunque este es solo un paso, consideramos que los artículos propuestos llenaran las lagunas legales existentes, y que además impedirán la impunidad de los ciberdelincuentes al fortalecer nuestra legislación.

No podemos dejar de señalar que nuestro país es signatario del Convenio de Budapest sobre la Ciberdelincuencia, que establece a las partes la obligación de adoptar las medidas legislativas que sean necesarias para combatir estos delitos, constituyendo el Anteproyecto de Ley que hoy presentamos a esta augusta cámara, *Que modifica y adiciona artículos al Código Penal sobre Delitos Informáticos*, un avance en la dirección correcta para el cumplimento de los compromisos adquiridos.

Honorables Diputados, por la importancia que reviste para nuestra sociedad combatir este flagelo, que muchas personas ya experimentan por haber sido afectadas por delitos informáticos, así como por la responsabilidad que me compete como Diputada de la República, de coadyuvar con las autoridades competentes para la persecución y sanción de los distintos tipos de delitos informáticos, les solicito su apoyo para que esta iniciativa legislativa cumpla el trámite legislativo y se convierta en Ley de la República.

ARLENA M. COBA M.
Diputada de la República
Circuito 4-3

ANTEPROYECTO DE LEY N°087
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

PROYECTO DE LEY No.

De de de 2024

Que modifica y adiciona artículos al Código Penal sobre Delitos Informáticos

LA ASAMBLEA NACIONAL

DECRETA:

Artículo 1. Se modifica el artículo 151 del Código Penal, así:

Artículo 151. Quien, mediante violencia, intimidación o amenaza grave, para procurarse o procurar a un tercero un lucro indebido o cualquier otro beneficio, obligue a otra persona a tomar una disposición patrimonial, a proporcionar información o a tolerar, hacer u omitir alguna cosa que le perjudique o perjudique a un tercero, será sancionado con prisión de cinco a diez años.

Esta sanción se incrementará en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica y cuando el delito emplee, imágenes, audios o videos de contenido sexual íntimo.

Artículo 2. Se adiciona el artículo 168-A del Código Penal, así:

Artículo 168-A. Las sanciones aplicables a los Delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad, se incrementarán en una mitad, cuando la acción se haya realizado mediante el uso de las tecnologías de la información y la comunicación por la que se exponga, distribuya, difunda, exhiba, trasmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización, y que le cause daño sicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

Artículo 3. Se adiciona el artículo 168-B del Código Penal, así:

Artículo 168-B. Quien, habiendo recibido las imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización a través del uso de tecnologías de la información y la comunicación, las difunda por los mismos medios, será sancionado con pena de multa/privación de libertad de tres meses a un año.

Artículo 4. Se adiciona el artículo 178-A del Código Penal, así:

> **Artículo 178-A.** Quien acose, hostigue o amenace a una persona mediante el uso de las tecnologías de la información y la comunicación será sancionado con pena de dos a cuatro años de prisión y tratamiento terapéutico multidisciplinario.
>
> Cuando exista relación jerárquica derivada de relaciones laborales, docentes, domésticas de cualquier clase que implique subordinación entre la persona agresora y la víctima, la pena se incrementará en una tercera parte.
>
> Si el autor fuese un servidor público, además de la pena prevista se le destituirá e inhabilitará para ocupar cargo en el sector público por igual término al de la pena de privación de la libertad impuesta.

Artículo 5. La presente Ley modifica el artículo 151 y adiciona los artículos 168-A, 168-B y 178-A Del Libro Segundo del Código Penal de la República de Panamá.

Artículo 6. Esta Ley empezará a regir el día siguiente a su promulgación.

COMUNÍQUESE Y CÚMPLASE

Propuesto a la consideración de la Asamblea Nacional, hoy de julio de 2024 por la Honorable Diputada

H.D. ARIANA M. COBA M.
Circuito 4-3

PROYECTO DE LEY Nº0050
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Presentación 27/8/24
Hora 5:49

Comisión de Gobierno, Justicia y Asuntos Constitucionales.

H.D. Luis Eduardo Camacho Castro
Presidente

Tel. (507) 512-8083
Fax. (507) 512-8120

Panamá, 27 de agosto de 2024.
2024_088_AN_CGJYAC.

Honorable Diputada
DANA CASTAÑEDA GUARDIA
Presidente de la Asamblea Nacional
Presente

Señora Presidente:

En cumplimiento del artículo 109 del Reglamento Orgánico del Régimen Interno de la Asamblea Nacional, debidamente analizado y prohijado por esta Comisión en su sesión del día 27 de agosto de 2024, remitimos el Proyecto de Ley **"Que modifica y adiciona artículos al código penal sobre delitos informáticos"**, que corresponde al Anteproyecto de Ley N° 87, originalmente presentado por la Honorable Diputada Ariana M. Coba M.

Le solicitamos se sirva impartir el trámite de rigor, con el objeto que la citada iniciativa legislativa sea sometida próximamente al primer debate.

Atentamente,

Luis Eduardo Camacho Castro
Presidente

LECC/RG/ep

EXPOSICIÓN DE MOTIVOS

Con el desarrollo de la internet se han roto barreras y se ha agilizado la comunicación en el mundo entero, dando paso a un sinnúmero de posibilidades para cada individuo al tener acceso a tanta información.

Esta disponibilidad se percibe en el gran número de usuarios de computadoras y otros dispositivos electrónicos existentes, que va en incremento al utilizarse no solo corno un medio de comunicación sino para realizar compras, pagos, para la enseñanza, la atención médica, entre algunos usos o aplicaciones que se le pueda dar.

Vernos que por el tipo y calidad de la información que se trasmite a través de la red, que incluye imágenes e información personal o comercial, en muchos casos confidencial, se ha despertado el interés de los denominados delincuentes cibernéticos, que no solo atacan los sistemas informáticos, sino que han ampliado su rango de acción, cometiendo delitos corno el fraude, la extorsión, la divulgación de información e imágenes sin autorización de la persona, amparados por incontables enlaces que les permiten actuar en el anonimato del mundo virtual o por darse la comisión en países donde no existe legislación sobre la materia o es muy escaza.

La escalada de los delitos informáticos en el mundo ha llevado a los países a desarrollar normativas para su prevención y sanción, corriente de la cual no escapa nuestro país.

Muchas son las denuncias que en los últimos años ha recibido el Ministerio Público, en especial las relacionadas con ataques a los sistemas informáticos, los de orden financiero, el acoso, hostigamiento y extorsión derivados de la violación de la privacidad y la violencia mediática, entre otros.

En ese sentido, en los últimos días se ha dado a conocer en las redes y medios de comunicación la comisión un delito informático de violación de la privacidad, que ha suscitado la repulsa de la sociedad y dejado claro, la necesidad de legislar sobre esta materia de manera más extensa para que la autoridad competente cuente con las herramientas para sancionar estos delitos, debido a que algunos de estos actos delictivos no se encuentran entre los tipos penales contenidos en el Código Penal vigente.

Atendiendo esa necesidad, presentamos esta iniciativa legislativa que contempla la modificación y adición de artículos al Código Penal vigente relativos a los delitos informáticos que desarrolla la extorsión, el acoso sexual, la violencia mediática y amplia los tipos penales de los artículos 289 al 292, que desarrollan delitos contra la seguridad informática, todo con la finalidad de contrarrestar los riesgos que estos generan para la sociedad, las empresas y los gobiernos.

También se hizo una revisión de las sanciones, aumentándose los años de prisión en algunos delitos, estableciendo las agravantes e incluyendo la inhabilitación para ejercer cargos públicos por el mismo tiempo de prisión.

Hacemos hincapié en los temas de violación de la intimidad de la persona y extorsión, porque es usual que quien se vea afectado por este tipo de violación, luego es forzado a dar, entregar o hacer algo para evitar que sus archivos sean trasmitidos por la red, para evitar así lo que se denomina violencia mediática.

Aunque este es solo un paso, consideramos que los artículos propuestos llenaran las lagunas legales existentes, y que además impedirán la impunidad de los ciberdelincuentes al fortalecer nuestra legislación.

No podemos dejar de señalar que nuestro país es signatario del Convenio de Budapest sobre la Ciberdelincuencia, que establece a las partes la obligación de adoptar las medidas legislativas que sean necesarias para combatir estos delitos, constituyendo el Anteproyecto de Ley que hoy presentamos a esta augusta cámara, *Que* mod~fica *y adiciona artículos al Código Penal sobre Delitos Informáticos,* un avance en la dirección correcta para el cumplimento de los compromisos adquiridos.

Honorables Diputados, por la importancia que reviste para nuestra sociedad combatir este flagelo, que muchas personas ya experimentan por haber sido afectadas por delitos informáticos, así como por la responsabilidad que me compete como Diputada de la República, de coadyuvar con las autoridades competentes para la persecución y sanción de los distintos tipos de delitos informáticos, les solicito su apoyo para que esta iniciativa legislativa cumpla el trámite legislativo y se convierta en Ley de la República.

PROYECTO DE LEY Nº0050
COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.

PROYECTO DE LEY N°

De de de 2024

Que modifica y adiciona artículos al Código Penal sobre Delitos Informáticos

LA ASAMBLEA NACIONAL

DECRETA:

Artículo 1. Se modifica el artículo 151 del Código Penal, así:

"**Artículo 151**. Quien, mediante violencia, intimidación o amenaza grave, para procurarse o procurar a un tercero un lucro indebido o cualquier otro beneficio, obligue a otra persona a tomar una disposición patrimonial, a proporcionar información o a tolerar, hacer u omitir alguna cosa que le perjudique o perjudique a un tercero, será sancionado con prisión de cinco a diez años.

Esta sanción se incrementará en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica y cuando el delito emplee, imágenes, audios o videos de contenido sexual íntimo.

Artículo 2. Se adiciona el artículo 168-A del Código Penal, así:

"**Artículo 168-A**. Las sanciones aplicables a los Delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad, se incrementarán en una mitad, cuando la acción se haya realizado mediante el uso de las tecnologías de la información y la comunicación por la que se exponga, distribuya, difunda, exhiba, trasmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización, y que le cause daño sicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

Artículo 3. Se adiciona el artículo 168-A del Código Penal, así:

"**Artículo 168-B**. Quien, habiendo recibido las imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización a través del uso de tecnologías de la información y la comunicación, las difunda por los mismos medios, será sancionado con pena de multa/privación de libertad de tres meses a un año.

Artículo 4. Se adiciona el artículo 178-A del Código Penal, así:

"**Artículo 178-A**. Quien acose, hostigue o amenace a una persona mediante el uso de las tecnologías de la información y la comunicación será sancionado con pena de dos a cuatro años de prisión y tratamiento terapéutico multidisciplinario.

Cuando exista relación jerárquica derivada de relaciones laborales, docentes, domésticas de cualquier clase que implique subordinación entre la persona agresora y la víctima, la pena se incrementará en una tercera parte.

Si el autor fuese un servidor público, además de la pena prevista se le destituirá e inhabilitará para ocupar cargo en el sector público por igual término al de la pena de privación de la libertad impuesta.

Artículo 5. La presente Ley modifica el artículo 151 y adiciona los artículos 168-A, 168-B y 178-A Del Libro Segundo del Código Penal de la República de Panamá.

Artículo 6. Esta Ley empezará a regir al día siguiente a su promulgación.

COMUNÍQUESE Y CÚMPLASE.

Proyecto de Ley propuesto a la consideración de la Asamblea Nacional, hoy ___ de agosto de 2024.

POR LA COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES

H.D. LUIS EDUARDO CAMACHO CASTRO
Presidente

H.D. ARIEL VALLARINO
Vicepresidente

H.D. FRANCISCO BREA
Secretario

H.D. CRISPIANO ADAMES NAVARRO
Comisionado

H.D. MANUEL CHENG
Comisionado

H.D. JOSÉ PÉREZ BARBONI
Comisionado

H.D. RAÚL PINEDA
Comisionado

H.D. DIDIANO PINILLA
Comisionado

H.D. ROBERTO ZÚÑIGA
Comisionado

I N F O R M E

Que rinde la Comisión de Gobierno, Justicia y Asuntos Constitucionales correspondiente al primer debate del **Proyecto de Ley N°61, " Por el cual se adoptan medidas contra la Ciberdelincuencia ".**

Panamá, 1de octubre de 2024.

Honorable Diputado
DANA CASTAÑEDA GUARDIA
Presidente
Asamblea Nacional
Presente.

Señor Presidente:

La Comisión de Gobierno, Justicia y Asuntos Constitucionales de la Asamblea Nacional en el marco de sus competencias funcionales consideró en su reunión de sesión ordinaria del día 5 de septiembre de 2024, conforme los trámites del Primer Debate reglamentario, el Proyecto de Ley N°61, **Por el cual se adoptan medidas contra la Ciberdelincuencia y se adoptan otras disposiciones ".**

En consecuencia y de acuerdo con el artículo 136 del Reglamento Orgánico del Régimen Interno de la Asamblea Nacional, rinde el informe correspondiente.

I. LA INICIATIVA LEGISLATIVA

Este Proyecto de Ley, fue presentado en la sesión ordinaria del día 5 de septiembre de 2024, por Procuraduría General de la Nación, y recibido en la Comisión de Gobierno como **Proyecto de Ley N° 61**, el 10 de septiembre de 2024 en cumplimiento con lo establecido en el artículo 109 del Reglamento Orgánico del Régimen Interno de la Asamblea Nacional.

II. CONTENIDO Y OBJETIVOS DEL PROYECTO

El Proyecto de Ley N° 61, consta de 36 artículos. Propone introducir nuevos tipos penales específicos para conductas delictivas que no estaban contempladas en la legislación vigente, tales como el uso de tecnología de la información, comunicación electrónica, abuso de dispositivos, interceptación ilícita de datos ataques, a la integridad de los sistemas, el acoso a los menores por vía cibernética, suplantación de identidad, disfunción no consentida, de material intimo y otros delitos relevantes.

Por otro lado, busca establecer, el derecho procesal los poderes necesarios para la investigación y el procesamiento de dichos delitos y un régimen eficaz de cooperación Internacional.

III. ANÁLISIS Y CONSIDERACIÓN DEL PROYECTO

El Proyecto de Ley N°61, fue objeto de un amplio análisis y estudio por parte de los miembros de esta Comisión.

Todos estos aspectos fueron explicados a los miembros de nuestra Comisión y revisados por el equipo técnico, lo cual conllevó a considerar viable su aprobación, por lo que se recomendó el trámite del Primer Debate.

El objetivo del mismo es la adecuación de la legislación nacional al Convenio de Budapest, adoptado por el Consejo de Europa en 2001 y aprobado por la República de Panamá mediante la Ley 79 del 22 de octubre de 2013, así como la incorporación de las tendencias modernas en la lucha contra la ciberdelincuencia e introducir nuevos tipos penales específicos para conductas delictivas que no estaban contempladas en la legislación vigente.

IV. DE LAS MODIFICACIONES.

En el presente proyecto de Ley, se consideró y aprobó, las modificaciones y adiciones, de los proyectos No 45, que establece políticas de prevención protección contra la violencia sexual digital y mediática, y el Proyecto de Ley No50, que modifica y adiciona articulo al Código Penal sobre delitos informáticos, **los cuales fueron unificados en primer debate**.

Todas estas modificaciones y adiciones, establecidas en este proyecto tienen el objetivo de hacer una realidad introducir nuevos tipos penales específicos para conductas delictivas que no estaban contempladas en la legislación vigente, relacionadas con la CIBERDELINCUENCIA para atender los conflictos que surgen producto del mal uso y abuso de esta tecnología.

V. EL PRIMER DEBATE

La Comisión de Gobierno, Justicia y Asuntos Constitucionales, el día 1 de octubre de 2024, aprobó en Primer Debate, con la mayoría de los miembros de dicha comisión, el Proyecto de Ley N°61, " **Por el cual se adoptan medidas contra la Ciberdelincuencia y se adoptan otras disposiciones ".**

Por todas las consideraciones anteriormente expresadas, la Comisión de Gobierno, Justicia y Asuntos Constitucionales, luego del exhaustivo estudio y en atención a la importancia que reviste el Proyecto de Ley N° 61.se dieron modificaciones de los artículos No 2,4, y del 25 al 34.

RESUELVE:

1. Aprobar en Primer Debate el Proyecto de Ley N°61, **Por el cual se adoptan medidas contra la Ciberdelincuencia y se adoptan otras disposiciones ". unificados con el proyecto de Ley** No 45, que establece políticas de prevención protección contra la violencia sexual digital y mediática, y el Proyecto de Ley No50, **que modifica y adiciona articulo al Código Penal Procesal sobre delitos informáticos, ",**

2. Presentar al Pleno en forma de texto único con las modificaciones en negrita y en numeración corrida
3. Recomendar al Pleno de la Asamblea Nacional que, le dé Segundo y Tercer Debate al Proyecto de Ley N°61, **Por el cual se adoptan medidas contra la Ciberdelincuencia y se adoptan otras disposiciones ".**

POR LA COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES

H.D. LUIS EDUARDO CAMACHO CASTRO
Presidente

H.D. ARIEL VALLARINO
Vicepresidente

H.D. FRANCISCO BREA
Secretario

H.D. CRISPIANO ADAMES
Comisionado

H.D. MANUEL CHENG
Comisionado

H.D. JOSÉ PÉREZ
Comisionado

H.D. RAÚL PINEDA
Comisionado

H.D. DIDIANO PINILLA
Comisionado

H.D. ROBERTO ZÚÑIGA
Comisionado

Proyecto 61

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
Presentación 2/10/24
Hora 6:32
A Debate
A Votación
Aprobada ____ Votos

TEXTO ÚNICO

Que contiene el Proyecto de Ley N° 61, **"Por el cual se adoptan medidas contra la Ciberdelincuencia y se dictan otras disposiciones".**

Panamá, 1 de octubre de 2024.

La Comisión de Gobierno, Justicia y Asuntos Constitucionales presenta al Pleno de la Asamblea Nacional el texto aprobado del Proyecto de Ley N° 61, **"Por el cual se adoptan medidas contra la Ciberdelincuencia y se dictan otras disposiciones",** arriba enunciado, y recomienda el siguiente Texto Único que contiene las propuestas aprobadas en la comisión:

PROYECTO DE LEY N° 61

De de de 2024

Por el cual se adoptan medidas contra la Ciberdelincuencia y se dictan otras disposiciones

LA ASAMBLEA NACIONAL,

DECRETA:

Artículo 1. A los efectos de la presente Ley los términos a continuación tendrán el siguiente significado:

1. Sistema informático. Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
2. Datos informáticos. Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
3. Proveedor de servicios: a. Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático; y, b. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.
4. Datos relativos al tráfico. Todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.
5. Datos relativos a los abonados. cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

   a. El tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

   b. La identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de

prestación de servicio; y, c. Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

6. Datos relativos al contenido. Se entiende el contenido comunicativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o la información transmitida por la comunicación. Se trata de todo lo transmitido como parte de la comunicación que no sean datos relativos al tráfico.
7. Infraestructura crítica. Las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
8. Material de abuso sexual infantil. Comúnmente denominado pornografía infantil, se entiende cualquier representación, por cualquier medio, de un menor participando enactividades sexuales explícitas, reales o simuladas, o cualquier representación de los órganos sexuales de un menor para fines principalmente sexuales, además del uso de un menor para crear tal representación

9. **Ciberengaño Pederasta o Groo Ming**: forma delictiva de acoso, comportamiento realizado desde plataformas digitales por personas adultas, que buscan ganar la confianza de niños, niñas o adolescentes, mediante la utilización de una identidad falsa, fingiendo ser un chico o una chica, para intercambiar imágenes y conversaciones con contenido sexual. Estas personas buscan involucrar a sus víctimas en actos sexuales.
10. **Difusión de contenido íntimo sin consentimiento**: dar a conocer por cualquier medio, por cualquier vía y a cualquier persona o grupo de personas, contenido íntimo (particularmente erótico – sexual) de una persona, sin que ésta lo haya consentido o autorizado específica y explícitamente.
11. **Extorsión Sexual o Extorsión**: chantaje o extorsión en el que una persona es amenazada con la divulgación de imágenes, videos o información de carácter sexual o íntimo, a menos que acceda a cumplir con determinadas demandas, que pueden incluir dinero, más contenido íntimo, o actos sexuales.
12. **Tecnología de la Información y la Comunicación**: recursos, herramientas y programas utilizados para procesar, administrar y compartir información mediante diversos soportes tecnológicos.

Artículo 2: Se modifica el artículo 151 del Código Penal, así:

Artículo 151. Quien, mediante violencia, intimidación o amenaza grave, para procurarse o procurar a un tercero un lucro indebido o cualquier otro beneficio, obligue a otra persona a tomar una disposición patrimonial, a proporcionar información o a tolerar, hacer u omitir alguna cosa que le perjudique o perjudique a un tercero, será sancionado con prisión de cinco a diez años.

Esta sanción se incrementará en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica y cuando el delito emplee, imágenes, audios o videos de contenido sexual íntimo.

Artículo 3-Se adiciona el artículo 166A al Código Penal, así:

Artículo 166A. Quien difunda, produzca o comercialice contenido íntimo, sexual o de desnudez, en el que se expongan imágenes, impresiones gráficas, audios o videos, reales o simulados, de una persona sin su consentimiento, sin su aprobación o sin su autorización, mediante el uso de tecnologías de la información y la comunicación, así como de cualquier otro medio, será sancionado con una pena de tres a seis años de prisión.

La pena será aumentada de una tercera parte a la mitad cuando las conductas descritas en el párrafo anterior se cometan:

1. Por una persona que esté o haya estado unida a la víctima por matrimonio, unión con vivencial o similar relación de afectividad, aún sin convivencia.

2. Con fines de lucro.

3. Por placer, codicia, odio racial, religioso o político.

4. Contra una persona con discapacidad; adulta mayor o persona en estado de inconciencia.

5. Por medio de cuentas falsas para ocultar la verdadera identidad del agresor

6. Cuando el autor se apodere u obtenga dicho contenido indebidamente.

Artículo 4. El artículo 184 del Código Penal, queda así:

Artículo 184. Quien fabrique, elabore por cualquier medio o produzca material de abuso sexual infantil o 10 ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de un medio de transferencia de datos, sistema informático, datos informáticos, programas maliciosos o cualquier tecnología emergente o cualquier medio de comunicación o información nacional o internacional, presentando o representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de diez a quince años.

La pena será de quince a veinte años de prisión si la víctima es una persona menor de catorce años o personas con capacidades especiales, si el autor pertenece a una organización criminal nacional o internacional o si el acto se realiza con ánimo de lucro.

Artículo 5. Se adiciona el artículo 184-A al Código Penal, así:

Artículo 184-A. Quien, con la finalidad de cometer delitos Contra la Libertad e Integridad Sexual, utilice cualquier medio, inclusive un sistema informático, sistema o comunicación electrónicos para contactarse o comunicarse con una persona menor de edad o persona con **Discapacidad** que no le permita resistirse, será sancionado con

pena de prisión de dos a cuatro años. La pena será de cuatro a seis años de prisión si la víctima es una persona menor de catorce años.

Artículo 6. El artículo 185 del Código Penal, queda así:

Artículo 185. Quien posea para su propio uso material de abuso sexual infantil o que contenga la imagen, real o simulada, de personas menores de edad, voluntariamente adquirido, será sancionado con pena de prisión de cinco a diez años. La pena será aumentada de una sexta parte a un tercio cuando se utilicen sistemas informáticos o medios de almacenamiento electrónico o redes sociales.

La pena será aumentada de una sexta parte a un tercio cuando se utilicen sistemas informáticos o medios de almacenamiento electrónico o redes sociales.

Artículo 7. Se adiciona el artículo 226-A al Código Penal, así:

Artículo 226-A. Quien suplante la identidad de una persona, para procurarse para sí o para un tercero un provecho ilícito, utilizando datos informáticos contenidos en una base de datos o un sistema informático, sistema electrónico, o adquiridos de cualquier otra forma, será sancionado con pena de dos a cuatro años de prisión.
Cuando la conducta cause un daño económico superior a los veinte mil balboas (B/. 20,000.00) la pena se aumentará a la mitad.

Artículo 8. Se adiciona el artículo 289-A al Código Penal, así:

Artículo 289-A. Quien, indebidamente, por medios técnicos, intercepte, interrumpa o interfiera datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, será sancionado con prisión de dos a cuatro años de prisión.

Artículo 9. El artículo 290 del Código Penal, queda así:

Artículo 290. Quien indebidamente se apodere, copie, utilice, modifique, dañe, borre, deteriore, altere o suprima datos informáticos, en tránsito o contenidos en una base de datos o sistema informático, será sancionado con dos a cuatro años de prisión.

Si la conducta descrita en el párrafo anterior causa un daño grave al titular de los datos informáticos la sanción se aumentará de un tercio a una sexta parte.

Artículo 10. Se adiciona el artículo 290-A al Código Penal, así:

Artículo 290-A. Quien indebidamente obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, será sancionado con dos a cuatro años de prisión.

Artículo 11. El artículo 291 del Código Penal, queda así:

Artículo 291. Las conductas descritas en éste Capítulo se agravarán de un tercio a una sexta parte de la pena si se cometen contra un sistema informático, sistema electrónico, datos informáticos de:

1. Oficinas públicas o bajo su tutela.
2. Instituciones públicas, privadas o mixtas que prestan un servicio público.
3. Bancos, aseguradoras y demás instituciones financieras y bursátiles.
4. Hospitales o cualquier tipo de entidad que maneje información relativa a datos médicos.
5. Sistemas informáticos o similares pertenecientes a infraestructura crítica o sistemas gubernamentales.

También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos con fines lucrativos o infringiendo medidas de seguridad.
Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV, del Libro Segundo de este Código.

Artículo 12. Se adiciona el artículo 292-A al Código Penal, así:

Artículo 292-A. Quien produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición cualquier dispositivo, incluido un programa informático, concebido o adaptado para la comisión de delitos a los que se refiere el presente capítulo, a sabiendas de su finalidad, será sancionado con dos a cuatro años de prisión.

Igual sanción se aplicará a quien obtenga o difunda una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con el fin de cometer delito.

No se considera delito la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el presente artículo que no tenga por objeto la comisión de uno de los delitos previstos en el Código Penal, ni tampoco la divulgación de datos informáticos o documentos

indispensables para la comprensión de la historia, las ciencias, las artes o cualquier información que sea de interés público.

Artículo 13. Se adiciona el artículo 428-A al Código Penal, así:

Artículo 428-A. Quien suplante la identidad de una persona, con el fin de obtener información confidencial o de seguridad del Estado, la pena será de cuatro a seis años.

Artículo 14. El numeral 1 del artículo 112 del Código Procesal Penal, queda así:

Artículo 112. Acción pública dependiente de instancia privada. ...

1. Delitos de difusión no consentida de material íntimo, acoso sexual y abusos deshonestos, cuando la víctima sea mayor de edad.
2. ...

Artículo 15. Se adiciona el artículo 314-A al Código Procesal Penal, así:

Artículo 314-A. Registro e incautación de datos informáticos almacenados. El Ministerio Público, en el marco de las investigaciones, podrá registrar o tener acceso a un sistema informático o a parte de este, así como incautar los datos informáticos en él almacenados.

En el caso en que tengan motivos para creer que los datos buscados se encuentran almacenados en otro sistema informático o en una parte del mismo, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, pueden extender el registro o el acceso de un modo similar al otro sistema.

En aplicación del presente artículo, se podrá obtener y conservar una copia de los datos informáticos y preservar su integridad. De ser necesario, se dispondrá a hacerlos inaccesibles o suprimirlos en el sistema informático consultado.

Artículo 16. Se adiciona el Capítulo VI al Título I del Libro Tercero del Código Procesal Penal, así:

Capítulo VI

Evidencia Digital

Artículo 17. Se adiciona el artículo 338-A al Código Procesal Penal, así:

Artículo 338-A. Conservación rápida de datos informáticos almacenados. El Ministerio Público podrá ordenar, a cualquier persona natural o jurídica, la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, que se encuentren en su poder o bajo su control, así como la protección de su integridad, cuando existan

motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. Esta medida no podrá exceder de noventa días, prorrogables por igual término, siempre que se mantengan las condiciones que motivaron su disposición.

La persona que custodia los datos o quien se encuentre encargada de su conservación estará obligada a mantener la reserva de la ejecución de la medida.

Artículo 18: Se adiciona el artículo 338-B al Código Procesal Penal, así:

Artículo 338-B. Conservación y revelación rápida de los datos relativos al tráfico. El Ministerio Público podrá ordenar a los proveedores de servicios, que hayan participado en la transmisión, la conservación rápida de los datos relativos al tráfico.

Si el proveedor requerido advierte que, en la comunicación, objeto de la investigación, han participado otros proveedores, deberá revelar rápidamente los datos que permitan identificar a todos los proveedores de servicio como la vía por la cual se transmitió la comunicación.

Artículo 19. Se adiciona el artículo 338-C al Código Procesal Penal, así:

Artículo 338-C. Orden de suministro. El Ministerio Público podrá ordenar a una persona, natural o jurídica, que suministre datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; o a un proveedor que ofrezca sus servicios en el territorio nacional, que suministre los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

Cuando el Ministerio Público logre la obtención de los datos correspondientes someterá los mismos al control posterior del Juez de Garantías, de conformidad con las reglas establecidas en este Código para la incautación de datos.

Artículo 20. Se adiciona el artículo 338-D al Código Procesal Penal, así:

Artículo 338-D. Obtención en tiempo real de datos relativos al tráfico y al contenido. Para la obtención o grabación, en tiempo real, de datos relativos al tráfico o relativos al contenido, por medios tecnológicos, se procederá conforme a lo establecido en el artículo 311 de este Código.

Para ello se podrá ordenar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas, su colaboración y su asistencia, quien deberá mantener la reserva de la medida.

Artículo 21. El artículo 4 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 4. Cuando la solicitud de asistencia jurídica no tenga fundamento en un convenio bilateral o multilateral del que la República de Panamá sea parte y se sustente en el principio de reciprocidad entre las naciones, corresponderá al Ministerio de Relaciones Exteriores recibir y remitir las solicitudes de asistencia jurídica vía diplomática. La viabilidad de la solicitud de asistencia jurídica presentada por el Estado requirente será determinada por la Procuraduría General de la Nación.

Artículo 22. Se adiciona el numeral 5 al artículo 6 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 6. ...

...

5. La asistencia se brindará conforme al principio de la doble incriminación, con independencia de que dicha conducta delictiva no se encuentre dentro de la misma categoría de delitos o se le denomine con una terminología distinta.

Artículo 23. El artículo 7 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 7. La asistencia jurídica internacional podrá solicitarse para:

1. La recepción de entrevistas, testimonios o declaraciones.
2. La remisión de documentos legales.
3. El examen de documentos, objetos y lugares.
4. La facilitación de información, elementos de pruebas y evaluaciones periciales.
5. La entrega de originales o copias certificadas de los documentos y expedientes pertinentes, incluida la documentación pública, bancaria o financiera, así como la documentación social o comercial de sociedades.
6. La identificación o localización del producto del delito, los bienes o activos lavados, procedentes de los instrumentos usados o que se pretenden usar en un acto delictivo o para la financiación del terrorismo, los bienes de valor equivalente u otros elementos con fines probatorios.
7. La facilitación de la comparecencia voluntaria de las personas al Estado requirente.
8. La autorización de la presencia, durante la ejecución de una solicitud, de las autoridades competentes de la Parte requirente o de sus delegados oficiales.
9. La aprehensión, incautación, embargo o comiso de bienes muebles e inmuebles, dineros, títulos, valores, bienes o activos producto del delito, procedentes de

instrumentos usados o que se pretenden usar en un acto delictivo o para la financiación del terrorismo y bienes de valor equivalente.

10. La realización de videoconferencias.

11. La entrega de antecedentes penales.

12. La búsqueda y localización de personas.

13. La realización de técnicas especiales de investigación como operaciones encubiertas, interceptación de comunicaciones, acceso a sistemas informáticos y entregas controladas.

14. La obtención de elementos de convicción y de pruebas de un delito en formato electrónico.

15. Otras formas de asistencia legal de conformidad con los fines de esta Ley, siempre que no sean incompatibles con las leyes nacionales.

Artículo 24. El artículo 8 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 8. Las solicitudes de asistencia jurídica podrán presentarse por escrito o por cualquier otro medio que deje constancia escrita, en condiciones que permitan a la autoridad central cerciorarse de su autenticad y transmisión segura.

Las autoridades centrales acordarán por escrito los canales seguros de transmisión y la forma de constatar la autenticidad.

Las autoridades centrales darán prioridad a los intercambios de solicitudes de asistencia jurídica, documentos adjuntos e información adicional entre las autoridades centrales por medios electrónicos.

En cualquier caso, previa solicitud y en cualquier momento se podrá solicitar la presentación de los documentos físicos en original o copia autenticada.

Artículo 25. El artículo 10 de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 10. Las solicitudes de asistencia jurídica internacional y demás documentos que con ella se envíen se presentarán traducidos al español en un idioma aceptado por la República de Panamá en un convenio bilateral o multilateral del que sea parte. Todos los documentos, registros, declaraciones y otros materiales en virtud de la presente Ley están exentos de cualquier requisito de legalización, autenticación y otras formalidades.

Artículo 26. Se adiciona el artículo 12-A de la Ley 11 de 31 de marzo de 2015, queda así:

Artículo 12-A. La autoridad competente, sin solicitud previa, podrá comunicar a otro Estado información obtenida en el marco de sus propias investigaciones penales cuando considere que la revelación de dicha información podría ayudar a dicho

Estado a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en su legislación interna, o podría dar lugar a una solicitud de cooperación de su parte.

Antes de comunicar dicha información, la autoridad competente podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones.

Artículo 27. Se adiciona el artículo 14 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-B. Se podrá denegar la asistencia si la solicitud se refiere a un delito que se considera delito político o delito vinculado a un delito político, o se considera que la ejecución de la solicitud podría atentar contra la soberanía, seguridad, orden público u otros intereses esenciales.

De igual forma, se podrá posponer la actuación en respuesta a una solicitud cuando pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por las autoridades.

En todo caso, antes de denegar o posponer la asistencia, se estudiará, previa consulta con el Estado requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que se consideren necesarias.

Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada.

También se informará al Estado requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

Artículo 28. Se adiciona el artículo 15 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-C: Cuando un Estado requirente solicite la conservación rápida de datos almacenados por medio de un sistema informático, el Ministerio Público podrá ordenarlo o asegurar los mismos de cualquier otra forma, de conformidad con las disposiciones establecidas en la legislación nacional.

Para los efectos del presente artículo, en las solicitudes de asistencia internacionales el Estado requirente indicará:

1. La autoridad que solicita dicha conservación;
2. El delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

3. Los datos informáticos almacenados que deben conservarse y su relación con el delito;
4. Cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;
5. La necesidad de la conservación, y
6. Que el Estado requirente tiene la intención de presentar una solicitud de asistencia jurídica internacional para el registro o el acceso de forma similar, la incautación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

Cuando el Estado panameño considere que la conservación por sí sola no sea suficiente para garantizar la futura disponibilidad de los datos, o ponga en peligro la confidencialidad de la investigación del Estado requirente o pueda causar cualquier otro perjuicio a la misma, informará de ello sin demora al solicitante, para que decida si debe, pese a ello, procederse a la ejecución de la medida.

Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el presente artículo tendrán una duración mínima de sesenta días, sin perjuicio de que se pueda conceder una prórroga hasta la presentación de la solicitud de asistencia jurídica internacional.

Artículo 29. Se adiciona el artículo 16 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-D. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo anterior para la conservación de datos sobre el tráfico en relación con una comunicación específica, la autoridad competente descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

Artículo 30. Se adiciona el artículo 17 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-E. Se prestará asistencia para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en el territorio transmitidas por medio de un sistema informático. Dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

De igual forma, se prestará la asistencia para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático, de conformidad con el derecho interno aplicable.

Artículo 31. Se adiciona el artículo 18 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-F. Se podrá diligenciar, una asistencia jurídica internacional con rapidez cuando se considere que existe una situación de emergencia, en la que exista un riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas.

Las solicitudes presentadas en virtud del presente artículo incluirán, además del contenido requerido, una descripción de los hechos que demuestren que existe una emergencia y cómo esta concierne a la asistencia solicitada.

Las peticiones en estos casos podrán ser transmitidas entre autoridades competentes, remitiéndose de forma simultánea una copia a la autoridad central del país requerido a través de la autoridad central del Estado requirente.

Las autoridades centrales acordarán por escrito los canales seguros de transmisión y la forma de constatar la autenticidad. Las autoridades competentes panameñas podrán solicitar con rapidez información complementaria para valorar la solicitud. De considerarse viable, se responderá oportunamente.

Previa solicitud del Estado requirente se podrán proporcionar los resultados de la ejecución de la solicitud o una copia, a través de un canal distinto del utilizado para la solicitud.

Para las situaciones de emergencia se garantizará que la autoridad central y la autoridad competente estén disponibles en todo momento habilitando los canales de comunicación correspondientes.

Artículo 32. Se adiciona el artículo 19 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-G. Se brindará asistencia para receptar el testimonio o declaraciones por videoconferencia o tecnología similar.

Las solicitudes de empleo de videoconferencia deben contener además de los requisitos establecidos en la presente Ley, el nombre y función de las autoridades del Estado requirente que participarán, las medidas relativas a la protección de la persona a ser oída, de ser necesario y cualquier aspecto relevante en relación a las condiciones para su ejecución.

La autoridad competente panameña y el Estado requirente procurarán facilitar la solución de cualquier problema que pueda surgir en relación con la ejecución de la solicitud de videoconferencia, de conformidad con la legislación interna del Estado requerido.

Las autoridades competentes procurarán que la persona cuyo testimonio o declaración se solicita comparezca en la fecha y horario acordado. La videoconferencia tendrá lugar en presencia de la autoridad competente panameña, se efectuará directamente por la autoridad competente del Estado requirente, o bajo su dirección, de conformidad con su legislación interna, y respetando los derechos y garantías previstos por ambos ordenamientos jurídicos.

Si la ejecución de la videoconferencia supone gastos de carácter extraordinario, se consultarán con el Estado requirente para determinar las condiciones en las que podrá ejecutarse la solicitud.

Artículo 33. Se adiciona el artículo 20 a la Ley 11 de 31 de marzo de 2015, así:

Artículo 12-H. Las autoridades competentes podrán crear Equipos Conjuntos de Investigación en relación con investigaciones penales, que, por su complejidad investigativa, ameriten una coordinación de acciones con otras jurisdicciones, a fin de lograr resultados más efectivos en la investigación, pudiendo intercambiar de forma directa, la evidencia a partir de su conformación de conformidad con las siguientes previsiones:

1. Las solicitudes de creación de Equipos Conjuntos de Investigación, deberán contener:
   a. Descripción de los motivos que ameritan la necesidad de su creación;
   b. Descripción de los procedimientos de investigación que se propongan realizar;
   c. Identificación de las autoridades competentes de la Parte Requirente para su integración; d. Plazo estimado de duración del Equipo Conjunto de Investigación; y,
   d. Los procedimientos que serán necesarios realizar, y
   e. Cualquier otra información necesaria.
2. Una vez acordada la creación del Equipo Conjunto de Investigación, las autoridades competentes a cargo de las investigaciones elaborarán y firmarán el respectivo Instrumento de creación y funcionamiento, que deberá contener entre otros aspectos los fines específicos, la composición, las funciones, la duración y prórrogas, la ubicación, organización, requisitos aplicables a la recopilación, transmisión y utilización de información o pruebas, cláusulas de confidencialidad y condiciones para la participación de las autoridades en las actividades de investigación que tengan lugar en el territorio de otro de los países que lo integran, de conformidad con sus respectivas legislaciones internas.
3. Una vez concluidas las funciones del Equipo Conjunto de Investigación se deberá elaborar un Acta de Terminación.

Artículo 34. Se adiciona el artículo 21 a la Ley 11 de 31 de marzo de 2015, así:

> **Artículo 12-I**. Los datos personales transmitidos al Estado requirente en virtud de solicitudes de asistencia jurídica internacional sólo podrán ser utilizados para los fines por los que fueron transmitidos y sujeto a las condiciones específicas debidamente motivadas establecidas por la autoridad que los transmitió. La utilización de los datos para otros fines por el Estado requirente necesita del consentimiento previo de la autoridad que los transmitió, teniendo en consideración la protección de los datos en su derecho interno.

Artículo 35. Se adiciona el artículo 22 a la Ley 11 de 31 de marzo de 2015, así:

> **Artículo 12-J**. En aquellos convenios o tratados internacionales en materia penal, en los que se establezcan redes permanentes para garantizar una asistencia inmediata, el punto de contacto será designado por el Procurador General de la Nación.

Artículo 36. La presente Ley modifica los artículos 151,184, 185, 290 y 291 del Código Penal; el artículo 112 del Código Procesal Penal; los artículos 4, 6, 7, 8, 10, de la Ley 11 de 31 de marzo de 2015; adiciona los artículos 166-A, 184-A, 226-A, 289-A, 290-A, 292-A al Código Penal; los artículos 314-A, 338-A, 338-B, 338-C y 338-D al Código Procesal Penal, 12-A,12-B,12-C,12-D,12-E,12-F,12-G,12-H,12-I,12-J, de la Ley 11 de 31 de marzo de 2015; así como también adiciona el Capítulo VI al Título I del Libro Tercero del Código Procesal Penal.

Artículo 37. Esta Ley entrará en vigencia a partir de su promulgación.

COMUNÍQUESE Y CÚMPLASE.

Proyecto de Ley propuesto a la consideración de la Asamblea Nacional, hoy ___ de octubre de 2024.

POR LA COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES

H.D. LUIS EDUARDO CAMACHO CASTRO
Presidente

H.D. ARIEL VALLARINO
Vicepresidente

H.D. FRANCISCO BREA
Secretario

H.D. CRISPIANO ADAMES
Comisionado

H.D. MANUEL CHENG
Comisionado

H.D. JOSÉ PÉREZ
Comisionado

H.D. RAÚL PINEDA
Comisionado

H.D. DIDIANO PINILLA
Comisionado

H.D. ROBERTO ZÚÑIGA
Comisionado

Proyecto 61

LEY

De de de 2024

Que modifica y adiciona artículos al Código Penal, al Código Procesal Penal y a la Ley 11 de 2015, sobre asistencia jurídica internacional en materia penal, y dicta otra disposición, respecto a medidas contra la ciberdelincuencia

LA ASAMBLEA NACIONAL

DECRETA:

Artículo 1. Para efectos de la aplicación de las medidas contra la ciberdelincuencia, los siguientes términos se entenderán así:

1. *Sistema informático.* Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función o la de alguno de sus elementos sea el tratamiento automatizado de datos en ejecución de un programa.
2. *Datos informáticos.* Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
3. *Proveedor de servicios.* Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, así como cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de este.
4. *Datos relativos al tráfico.* Cualesquier datos informáticos relativos a una comunicación realizada por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, y que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.
5. *Datos relativos a los abonados.* Cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permita determinar:
    a. El tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio.
    b. La identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio.
    c. Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.
6. *Datos relativos al contenido.* Contenido comunicativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o la información

transmitida por la comunicación. Se trata de todo lo transmitido como parte de la comunicación que no sean datos relativos al tráfico.

7. *Infraestructura crítica.* Las infraestructuras estratégicas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable en la seguridad económica, seguridad o salud pública y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un impacto sobre los servicios esenciales.
8. *Material de abuso sexual infantil.* Comúnmente denominado pornografía infantil. Cualquier representación, por cualquier medio, de un menor participando en actividades sexuales explícitas, reales o simuladas, o cualquier representación de los órganos sexuales de un menor para fines principalmente sexuales, además del uso de un menor para crear tal representación.
9. *Ciberengaño pederasta o grooming.* Forma delictiva de acoso, comportamiento realizado desde plataformas digitales por personas adultas que buscan ganar la confianza de niños, niñas o adolescentes, mediante la utilización de una identidad falsa, fingiendo ser un niño, niña o adolescente, para intercambiar imágenes y conversaciones con contenido sexual. Estas personas buscan involucrar a sus víctimas en actos sexuales.
10. *Difusión de contenido íntimo sin consentimiento.* Dar a conocer, por cualquier medio, por cualquier vía y a cualquier persona o grupo de personas, contenido íntimo (particularmente erótico-sexual) de una persona, sin que esta lo haya consentido o autorizado específica y explícitamente.
11. *Extorsión sexual o sextorsión.* Chantaje o extorsión con el que una persona es amenazada con la divulgación de imágenes, videos o información de carácter sexual o íntimo, a menos que acceda a cumplir con determinadas demandas, que pueden incluir dinero, más contenido íntimo o actos sexuales.
12. *Tecnologías de la información y la comunicación (TIC).* Recursos, herramientas y programas utilizados para procesar, administrar y compartir información mediante diversos soportes tecnológicos.

Artículo 2. El artículo 151 del Código Penal queda así:

Artículo 151. Quien, mediante violencia, intimidación o amenaza grave, para procurarse o procurar a un tercero un lucro indebido o cualquier otro beneficio, obligue a otra persona a tomar una disposición patrimonial, a proporcionar información o a tolerar, hacer u omitir alguna cosa que le perjudique o perjudique a un tercero, será sancionado con prisión de cinco a diez años.

La sanción se aumentará de un tercio a la mitad cuando se utilice como medio las tecnologías de la información y la comunicación y cuando el delito emplee imágenes, audios o videos de contenido sexual íntimo reales, simulados o generados.

Artículo 3. Se adiciona el artículo 166-A al Código Penal, así:

Artículo 166-A. Quien difunda, produzca o comercialice contenido íntimo, sexual o de desnudez, en el que se expongan imágenes, impresiones gráficas, audios o videos, reales o simulados, de una persona sin su consentimiento, sin su aprobación o sin su autorización, mediante el uso de tecnologías de la información y la comunicación, así como de cualquier otro medio, será sancionado con pena de tres a seis años de prisión.

La pena será aumentada de una tercera parte a la mitad cuando las conductas descritas en el párrafo anterior se cometan:

1. Por una persona que esté o haya estado unida a la víctima por matrimonio, unión de hecho o similar relación de afectividad, aun sin convivencia.
2. Con fines de lucro.
3. Por placer, codicia, odio racial, religioso o político.
4. Contra una persona con discapacidad, adulta mayor o en estado de inconsciencia.
5. Por medio de cuentas falsas para ocultar la verdadera identidad del agresor.
6. Apoderándose u obteniendo dicho contenido indebidamente.

Artículo 4. El artículo 184 del Código Penal queda así:

Artículo 184. Quien fabrique, elabore por cualquier medio o produzca material de abuso sexual infantil o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de un medio de transferencia de datos, sistema informático, datos informáticos, programas maliciosos o cualquier tecnología emergente o cualquier medio de comunicación o información nacional o internacional, presentando o representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de diez a quince años.

La pena será de quince a veinte años de prisión si la víctima es una persona menor de catorce años o persona con discapacidad, si el autor pertenece a una organización criminal nacional o internacional o si el acto se realiza con ánimo de lucro.

Artículo 5. Se adiciona el artículo 184-A al Código Penal, así:

Artículo 184-A. Quien, con la finalidad de cometer delitos contra la libertad e integridad sexual, utilice cualquier medio, inclusive un sistema informático o sistema o comunicación electrónico para contactarse o comunicarse con una persona menor de edad o persona con discapacidad que no le permita resistirse, será sancionado con pena de prisión de dos a cuatro años. La pena será de cuatro a seis años de prisión si la víctima es una persona menor de catorce años.

Artículo 6. El artículo 185 del Código Penal queda así:

Artículo 185. Quien posea para su propio uso material de abuso sexual infantil que contenga la imagen, real o simulada, de personas menores de edad, voluntariamente adquirido, será sancionado con pena de prisión de cinco a diez años.

La pena será aumentada de una sexta parte a un tercio cuando se utilicen sistemas informáticos o medios de almacenamiento electrónico o redes sociales.

Artículo 7. Se adiciona el artículo 289-A al Código Penal, así:

Artículo 289-A. Quien suplante la identidad de una persona, con fines ilícitos, utilizando datos informáticos, bases de datos o un sistema electrónico, o adquiriéndolos de cualquier otra forma, será sancionado con pena de dos a cuatro años de prisión.

Artículo 8. Se adiciona el artículo 289-A al Código Penal, así:

Artículo 289-B. Quien indebidamente, por medios tecnológicos, intercepte, interrumpa o interfiera datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro de este, será sancionado con prisión de dos a cuatro años de prisión.

Artículo 9. El artículo 290 del Código Penal queda así:

Artículo 290. Quien indebidamente se apodere, copie, utilice, modifique, dañe, borre, deteriore, altere o suprima datos informáticos, en tránsito o contenidos en una base de datos o sistema informático, será sancionado con dos a cuatro años de prisión.

Si la conducta descrita en el párrafo anterior causa un daño grave al titular de los datos informáticos, la sanción se aumentará de un tercio a una sexta parte.

Artículo 10. Se adiciona el artículo 290-A al Código Penal, así:

Artículo 290-A. Quien indebidamente obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, será sancionado con dos a cuatro años de prisión.

Artículo 11. El artículo 291 del Código Penal queda así:

Artículo 291. Las conductas descritas en este Capítulo se agravarán de un tercio a una sexta parte de la pena si se cometen contra un sistema informático, sistema electrónico o datos informáticos de:

1. Oficinas públicas o bajo su tutela.
2. Instituciones públicas, privadas o mixtas que prestan un servicio público.
3. Bancos, aseguradoras y demás instituciones financieras y bursátiles.

4. Hospitales o cualquier tipo de entidad que maneje información relativa a datos médicos.
5. Sistemas informáticos o similares pertenecientes a infraestructura crítica.

También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos con fines lucrativos o infringiendo medidas de seguridad.

Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente Capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I del Título XIV del Libro Segundo de este Código.

Artículo 12. Se adiciona el artículo 292-A al Código Penal, así:

Artículo 292-A. Quien produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición cualquier dispositivo, incluido un programa informático, concebido o adaptado para la comisión de delitos a los que se refiere el presente Capítulo, a sabiendas de su finalidad, será sancionado con dos a cuatro años de prisión.

Igual sanción se aplicará a quien obtenga o difunda una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con el fin de cometer delito.

Artículo 13. Se adiciona el artículo 428-A al Código Penal, así:

Artículo 428-A. Quien suplante la identidad de una persona, con el fin de obtener información confidencial o de seguridad del Estado, la pena será de cuatro a seis años prisión.

Artículo 14. El numeral 1 del artículo 112 del Código Procesal Penal queda así:

Artículo 112. Acción pública dependiente de instancia privada. …

Son delitos de acción pública dependiente de instancia privada los siguientes:

1. Delitos de difusión no consentida de material íntimo, acoso sexual y abusos deshonestos, cuando la víctima sea mayor de edad.

…

Artículo 15. Se adiciona el artículo 314-A al Código Procesal Penal, así:

Artículo 314-A. Registro e incautación de datos informáticos almacenados. El Ministerio Público, en el marco de las investigaciones, podrá registrar o tener acceso a un sistema informático o a parte de este, así como incautar los datos informáticos en él almacenados.

En caso de que tenga motivos para creer que los datos buscados se encuentran almacenados en otro sistema informático o en una parte de este, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio

de dicho sistema inicial, podrá extender el registro o el acceso de un modo similar al otro sistema.

En aplicación del presente artículo, se podrá obtener y conservar una copia de los datos informáticos y preservar su integridad. De ser necesario, se dispondrá a hacerlos inaccesibles o suprimirlos en el sistema informático consultado.

Artículo 16. Se adiciona el Capítulo VI, contentivo de los artículos 338-A, 338-B, 338-C y 338-D, al Título I del Libro Tercero del Código Procesal Penal, así:

Capítulo VI
Evidencia Digital

Artículo 338-A. Conservación rápida de datos informáticos almacenados. El Ministerio Público podrá ordenar, a cualquier persona natural o jurídica, la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, que se encuentren en su poder o bajo su control, así como la protección de su integridad, cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. Esta medida no podrá exceder de noventa días, prorrogables por igual término, siempre que se mantengan las condiciones que motivaron su disposición.

La persona que custodia los datos o quien se encuentre encargada de su conservación estará obligada a mantener la reserva de la ejecución de la medida.

Artículo 338-B. Conservación y revelación rápida de los datos relativos al tráfico. El Ministerio Público podrá ordenar a los proveedores de servicios que hayan participado en la transmisión la conservación rápida de los datos relativos al tráfico.

Si el proveedor requerido advierte que en la comunicación objeto de la investigación han participado otros proveedores, deberá revelar rápidamente los datos que permitan identificar a todos los proveedores de servicio, así como la vía por la cual se transmitió la comunicación.

Artículo 338-C. Orden de suministro. El Ministerio Público podrá ordenar a una persona natural o jurídica que suministre datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; o a un proveedor que ofrezca sus servicios en el territorio nacional, que suministre los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

Cuando el Ministerio Público logre la obtención de los datos correspondientes los someterá al control posterior del Juez de Garantías, de conformidad con las reglas establecidas en este Código para la incautación de datos.

Artículo 338-D. Obtención en tiempo real de datos relativos al tráfico y al contenido. Para la obtención o grabación, en tiempo real, de datos relativos al tráfico o relativos al contenido, por medios tecnológicos, se procederá conforme a lo establecido en el artículo 311 de este Código.

Para ello, se podrá ordenar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas, su colaboración y su asistencia, quien deberá mantener la reserva de la medida.

Artículo 17. El artículo 4 de la Ley 11 de 2015 queda así:

Artículo 4. Cuando la solicitud de asistencia jurídica no tenga fundamento en un convenio bilateral o multilateral del que la República de Panamá sea parte y se sustente en el principio de reciprocidad entre las naciones, corresponderá al Ministerio de Relaciones Exteriores recibir y remitir las solicitudes de asistencia jurídica vía diplomática. La viabilidad de la solicitud de asistencia jurídica presentada por el Estado requirente será determinada por la Procuraduría General de la Nación.

Artículo 18. Se adiciona el numeral 5 al artículo 6 de la Ley 11 de 2015, así:

Artículo 6. Las solicitudes de asistencia internacional en materia penal conforme a esta Ley tendrán el alcance siguiente:

...

5. La asistencia se brindará conforme al principio de la doble incriminación, con independencia de que dicha conducta delictiva no se encuentre dentro de la misma categoría de delitos o se le denomine con una terminología distinta.

Artículo 19. El artículo 7 de la Ley 11 de 2015 queda así:

Artículo 7. La asistencia jurídica internacional podrá solicitarse para:

1. La recepción de entrevistas, testimonios o declaraciones.
2. La remisión de documentos legales.
3. El examen de documentos, objetos y lugares.
4. La facilitación de información, elementos de pruebas y evaluaciones periciales.
5. La entrega de originales o copias certificadas de los documentos y expedientes pertinentes, incluida la documentación pública, bancaria o financiera, así como la documentación social o comercial de sociedades.
6. La identificación o localización del producto del delito, los bienes o activos lavados, procedentes de los instrumentos usados o que se pretenden usar en un acto delictivo o para la financiación del terrorismo, los bienes de valor equivalente u otros elementos con fines probatorios.
7. La facilitación de la comparecencia voluntaria de las personas al Estado requirente.

8. La autorización de la presencia, durante la ejecución de una solicitud, de las autoridades competentes de la Parte requirente o de sus delegados oficiales.
9. La aprehensión, incautación, embargo o comiso de bienes muebles e inmuebles, dineros, títulos, valores, bienes o activos producto del delito, procedentes de instrumentos usados o que se pretenden usar en un acto delictivo o para la financiación del terrorismo y bienes de valor equivalente.
10. La realización de videoconferencias.
11. La entrega de antecedentes penales.
12. La búsqueda y localización de personas.
13. La realización de técnicas especiales de investigación como operaciones encubiertas, interceptación de comunicaciones, acceso a sistemas informáticos y entregas controladas.
14. La obtención de elementos de convicción y de pruebas de un delito en formato electrónico.
15. Otras formas de asistencia legal de conformidad con los fines de esta Ley, siempre que no sean incompatibles con las leyes nacionales.

Artículo 20. El artículo 8 de la Ley 11 de 2015 queda así:

Artículo 8. Las solicitudes de asistencia jurídica podrán presentarse por escrito o por cualquier otro medio que deje constancia escrita, en condiciones que permitan a la autoridad central cerciorarse de su autenticidad y transmisión segura.

Las autoridades centrales acordarán por escrito los canales seguros de transmisión y la forma de constatar la autenticidad.

Las autoridades centrales darán prioridad a los intercambios de solicitudes de asistencia jurídica, documentos adjuntos e información adicional entre las autoridades centrales por medios electrónicos.

En cualquier caso, previa solicitud y en cualquier momento, se podrá solicitar la presentación de los documentos físicos en original o copia autenticada.

Artículo 21. El artículo 10 de la Ley 11 de 2015 queda así:

Artículo 10. Las solicitudes de asistencia jurídica internacional y demás documentos que con ella se envíen se presentarán traducidos al español o en un idioma aceptado por la República de Panamá en un convenio bilateral o multilateral del que sea parte. Todos los documentos, registros, declaraciones y otros materiales en virtud de la presente Ley están exentos de cualquier requisito de legalización, autenticación y otras formalidades.

Artículo 22. Se adiciona el artículo 12-A a la Ley 11 de 2015, así:

Artículo 12-A. La autoridad competente, sin solicitud previa, podrá comunicar a otro Estado información obtenida en el marco de sus propias investigaciones penales

cuando considere que la revelación de dicha información podría ayudar a dicho Estado a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en su legislación interna, o podría dar lugar a una solicitud de cooperación de su parte.

Antes de comunicar dicha información, la autoridad competente podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones.

Artículo 23. Se adiciona el artículo 12-B a la Ley 11 de 2015, así:

Artículo 12-B. Se podrá denegar la asistencia si la solicitud se refiere a un delito que se considera delito político o delito vinculado a un delito político, o se considera que la ejecución de la solicitud podría atentar contra la soberanía, seguridad, orden público u otros intereses esenciales.

De igual forma, se podrá posponer la actuación en respuesta a una solicitud cuando pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por las autoridades.

En todo caso, antes de denegar o posponer la asistencia, se estudiará, previa consulta con el Estado requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que se consideren necesarias.

Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada.

También se informará al Estado requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

Artículo 24. Se adiciona el artículo 12-C a la Ley 11 de 2015, así:

Artículo 12-C. Cuando un Estado requirente solicite la conservación rápida de datos almacenados por medio de un sistema informático, el Ministerio Público podrá ordenarlo o asegurar los datos de cualquier otra forma, de conformidad con las disposiciones establecidas en la legislación nacional.

Para los efectos del presente artículo, en las solicitudes de asistencia internacionales el Estado requirente indicará:

1. La autoridad que solicita dicha conservación.
2. El delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el delito.
3. Los datos informáticos almacenados que deben conservarse y su relación con el delito.
4. Cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático.
5. La necesidad de la conservación.

6. Que el Estado requirente tiene la intención de presentar una solicitud de asistencia jurídica internacional para el registro o el acceso de forma similar, la incautación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

Cuando el Estado panameño considere que la conservación por sí sola no sea suficiente para garantizar la futura disponibilidad de los datos, o ponga en peligro la confidencialidad de la investigación del Estado requirente o pueda causar cualquier otro perjuicio a esta, informará de ello sin demora al solicitante, para que decida si debe, pese a ello, procederse a la ejecución de la medida.

Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el presente artículo tendrán una duración mínima de sesenta días, sin perjuicio de que se pueda conceder una prórroga hasta la presentación de la solicitud de asistencia jurídica internacional.

Artículo 25. Se adiciona el artículo 12-D a la Ley 11 de 2015, así:

Artículo 12-D. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo anterior para la conservación de datos sobre el tráfico en relación con una comunicación específica, la autoridad competente descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

Artículo 26. Se adiciona el artículo 12-E a la Ley 11 de 2015, así:

Artículo 12-E. Se prestará asistencia para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en el territorio transmitidas por medio de un sistema informático. Dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

De igual forma, se prestará la asistencia para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático, de conformidad con el derecho interno aplicable.

Artículo 27. Se adiciona el artículo 12-F a la Ley 11 de 2015, así:

Artículo 12-F. Se podrá diligenciar una asistencia jurídica internacional con rapidez cuando se considere que existe una situación de emergencia, en la que exista un riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas.

Las solicitudes presentadas en virtud del presente artículo incluirán, además del contenido requerido, una descripción de los hechos que demuestren que existe una emergencia y cómo esta concierne a la asistencia solicitada.

Las peticiones en estos casos podrán ser transmitidas entre autoridades competentes, remitiéndose de forma simultánea una copia a la autoridad central del país requerido a través de la autoridad central del Estado requirente.

Las autoridades centrales acordarán por escrito los canales seguros de transmisión y la forma de constatar la autenticidad. Las autoridades competentes panameñas podrán solicitar con rapidez información complementaria para valorar la solicitud. De considerarse viable, se responderá oportunamente.

Previa solicitud del Estado requirente, se podrán proporcionar los resultados de la ejecución de la solicitud o una copia, a través de un canal distinto del utilizado para la solicitud.

Para las situaciones de emergencia, se garantizará que la autoridad central y la autoridad competente estén disponibles en todo momento, habilitando los canales de comunicación correspondientes.

Artículo 28. Se adiciona el artículo 12-G a la Ley 11 de 2015, así:

Artículo 12-G. Se brindará asistencia para receptar el testimonio o declaraciones por videoconferencia o tecnología similar.

Las solicitudes de empleo de videoconferencia deben contener, además de los requisitos establecidos en la presente Ley, el nombre y función de las autoridades del Estado requirente que participarán, las medidas relativas a la protección de la persona a ser oída, de ser necesario, y cualquier aspecto relevante con relación a las condiciones para su ejecución.

La autoridad competente panameña y el Estado requirente procurarán facilitar la solución de cualquier problema que pueda surgir con relación a la ejecución de la solicitud de videoconferencia, de conformidad con la legislación interna del Estado requerido.

Las autoridades competentes procurarán que la persona cuyo testimonio o declaración se solicita comparezca en la fecha y horario acordado. La videoconferencia tendrá lugar en presencia de la autoridad competente panameña, se efectuará directamente por la autoridad competente del Estado requirente o bajo su dirección, de conformidad con su legislación interna, y respetando los derechos y garantías previstos por ambos ordenamientos jurídicos.

Si la ejecución de la videoconferencia supone gastos de carácter extraordinario, se consultarán con el Estado requirente para determinar las condiciones en las que podrá ejecutarse la solicitud.

Artículo 29. Se adiciona el artículo 12-H a la Ley 11 de 2015, así:

Artículo 12-H. Las autoridades competentes podrán crear equipos conjuntos de investigación en relación con investigaciones penales que, por su complejidad investigativa, ameriten una coordinación de acciones con otras jurisdicciones, a fin

de lograr resultados más efectivos en la investigación, pudiendo intercambiar de forma directa la evidencia a partir de su conformación, de acuerdo con las siguientes previsiones:

1. Las solicitudes de creación de equipos conjuntos de investigación deberán contener:
    a. Descripción de los motivos que ameritan la necesidad de su creación.
    b. Descripción de los procedimientos de investigación que se propongan realizar.
    c. Identificación de las autoridades competentes de la Parte requirente para su integración.
    d. Plazo estimado de duración del equipo conjunto de investigación.
    e. Los procedimientos que serán necesarios realizar.
    f. Cualquier otra información necesaria.
2. Una vez acordada la creación del equipo conjunto de investigación, las autoridades competentes a cargo de las investigaciones elaborarán y firmarán el respectivo instrumento de creación y funcionamiento, que deberá contener, entre otros aspectos, los fines específicos, la composición, las funciones, la duración y prórrogas, la ubicación, la organización, los requisitos aplicables a la recopilación, la transmisión y utilización de información o pruebas, las cláusulas de confidencialidad y las condiciones para la participación de las autoridades en las actividades de investigación que tengan lugar en el territorio de otro de los países que lo integran, de conformidad con sus respectivas legislaciones internas.
3. Una vez concluidas las funciones del equipo conjunto de investigación, se deberá elaborar un acta de terminación.

Artículo 30. Se adiciona el artículo 12-I a la Ley 11 de 2015, así:

Artículo 12-I. Los datos personales transmitidos al Estado requirente en virtud de solicitudes de asistencia jurídica internacional solo podrán ser utilizados para los fines por los que fueron transmitidos y sujeto a las condiciones específicas debidamente motivadas establecidas por la autoridad que los transmitió. La utilización de los datos para otros fines por el Estado requirente necesita del consentimiento previo de la autoridad que los transmitió, teniendo en consideración la protección de los datos en su derecho interno.

Artículo 31. Se adiciona el artículo 12-J a la Ley 11 de 2015, así:

Artículo 12-J. En aquellos convenios o tratados internacionales en materia penal, en los que se establezcan redes permanentes para garantizar una asistencia inmediata, el punto de contacto será designado por el procurador general de la nación.

Artículo 32. La presente Ley modifica los artículos 151, 184, 185, 290 y 291 y adiciona los artículos 166-A, 184-A, 289-A, 289-B, 290-A, 292-A y 428-A al Código Penal; modifica el numeral 1 del artículo 112 y adiciona el artículo 314-A y el Capítulo VI, contentivo de los artículos 338-A, 338-B, 338-C y 338-D, al Título I del Libro Tercero del Código Procesal Penal, y modifica los artículos 4, 7, 8 y 10 y adiciona el numeral 5 al artículo 6 y los artículos 12-A, 12-B, 12-C, 12-D, 12-E, 12-F, 12-G, 12-H, 12-I y 12-J a la Ley 11 de 31 de marzo de 2015.

Artículo 33. Esta Ley comenzará a regir desde su promulgación.

COMUNÍQUESE Y CÚMPLASE.

Proyecto 61 de 2024 aprobado en tercer debate en el Palacio Justo Arosemena, ciudad de Panamá, a los nueve días del mes de octubre del año dos mil veinticuatro.

La Presidenta,

Dana Castañeda Guardia

El Secretario General,

Carlos Alvarado González

PRESIDENCIA
27NOV2024AM11:49
ASAMBLEA NACIONAL

República de Panamá

Presidencia

ASAMBLEA NACIONAL
Secretaría General
RECIBIDO
Por: SJK
Fecha: 27/11/24 Hora: 12:02 P.M.

19 de noviembre de 2024
Nota No. 745-2024-AL

Honorable Diputada
DANA CASTAÑEDA
Presidenta de la Asamblea Nacional
E. S. D.

Señora presidenta:

Me es grato dirigirme a usted, actuando en ejercicio de la facultad que me confiere el numeral 6 del artículo 183 de la Constitución Política de la República, en concordancia con el párrafo primero del artículo 169 del mismo Texto Constitucional, en ocasión de devolver a esa augusta Cámara, sin haber sido objeto de sanción, el **Proyecto de Ley 61 de 2024, Que modifica y adiciona artículos al Código Penal, al Código Procesal Penal y a la Ley 11 de 2015, sobre asistencia jurídica internacional en materia penal, y dicta otra disposición, respecto a medidas contra la ciberdelincuencia;** habida cuenta que, al proceder al análisis de las opiniones recibidas por parte del Ministerio de Relaciones Exteriores, el Ministerio de Comercio e Industrias, el Ministerio de Economía y Finanzas, la Procuraduría General de la Nación y la Autoridad Nacional para la Innovación Gubernamental, he encontrado razones que me permiten objetar parcialmente, los artículos 3, 7, 12 y 16, por inconvenientes e inexequibles en los términos que a continuación paso a expresar.

A. De la objeción parcial, por inconveniencia

1. Se objeta, por inconveniente, el artículo 3 del Proyecto de Ley 61 de 2024, cuyo texto es el siguiente:

Artículo 3. Se adiciona el artículo 166-A al Código Penal, así:

> **Artículo 166-A.** Quien difunda, produzca o comercialice contenido íntimo, sexual o de desnudez, en el que se expongan

imágenes, impresiones gráficas, audios o videos, reales o simulados, de una persona sin su consentimiento, sin su aprobación o sin su autorización, mediante el uso de tecnologías de la información y la comunicación, así como de cualquier otro medio, será sancionado con pena de tres a seis años de prisión.

La pena será aumentada de una tercera parte a la mitad cuando las conductas descritas en el párrafo anterior se cometan:

1. Por una persona que esté o haya estado unida a la víctima por matrimonio, unión de hecho o similar relación de afectividad, aun sin convivencia.
2. Con fines de lucro.
3. Por placer, codicia, odio racial, religioso o político.
4. Contra una persona con discapacidad, adulta mayor o en estado de inconsciencia.
5. Por medio de cuentas falsas para ocultar la verdadera identidad del agresor.
6. Apoderándose u obteniendo dicho contenido indebidamente.

La técnica de ubicación del tipo penal 166-A introducida al Código Penal del Proyecto de Ley 61, se adecúa más a un delito contra la dignidad, decoro u honor y no así a un delito contra la intimidad, esto, desde la óptica del bien jurídico tutelado. Lo anterior porque, una persona, al consentir grabarse, se despoja de esa intimidad, lo que coloca el uso de dicha grabación en un tema de dignidad y decoro, cuando la transmisión es la que no fue autorizada. Esta observación tiene relevancia cuando los delitos contra el honor, son delitos de acción privada, es decir, que requieren de querellas necesarias mas no así los que vulneran la intimidad, que son de acción pública dependientes de instancia privada, y su persecución oficiosa se da tan solo por la información brindada por la víctima.

2. Se objeta, por inconveniente, el artículo 7 del Proyecto de Ley 61 de 2024, cuyo texto es el siguiente:

Artículo 7. Se adiciona el artículo 289-A al Código Penal, así:

Artículo 289-A. Quien suplante la identidad de una persona, con fines ilícitos, utilizando datos informáticos, bases de datos o un sistema electrónico, o adquiriéndolos de cualquier otra forma, será sancionado de dos a cuatro años de prisión.

El artículo 289-A, que se adiciona al Código Penal mediante el artículo 7 del Proyecto de Ley 61, es inconveniente por existir una dualidad con el numeral 4 del artículo 221 del Código Penal, que lee así:

> **Artículo 221.** La conducta prevista en el artículo anterior será sancionada con prisión de cinco a diez años en los siguientes casos:
> 1. ...
> 4. Si se usurpa o utiliza la identidad de otra persona para obtener algún beneficio.

En el precepto punitivo citado, la usurpación o "suplantación de identidad" con fines ilícitos para obtener beneficios, ya está regulada con penalidad de cinco a diez años (modalidad de estafa agravada). Con el artículo 7 del Proyecto de Ley 61, se introducen otros elementos del mismo tipo penal ya existente, que sofistican la conducta, pero ilógicamente en lugar de agravar la pena se reduce a una sanción de dos a cuatro años de prisión.

Como puede observarse, se introducen los elementos: "*utilizando datos informáticos, bases de datos o un sistema electrónico, o adquiriéndolos de cualquier otra forma...*", lo que demuestra que la conducta es más elaborada, sin embargo, en una incongruencia legislativa, se disminuye pronunciadamente la penalidad, incumpliéndose con ello los fines propios de la pena regulados en el artículo 7 del Código Penal (efectos preventivos, disuasivos y de retribución acorde a lo cometido).

3. Se objeta, por inconveniente, el artículo 12 del Proyecto de Ley 61 de 2024, cuyo texto es el siguiente:

> **Artículo 12.** Se adiciona el artículo 292-A al Código Penal, así:
> **Artículo 292-A.** Quien produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición cualquier dispositivo, incluido un programa informático, **concebido o adaptado para la comisión de delitos** a los que se refiere el presente Capítulo, **a sabiendas de su finalidad**, será sancionado con dos a cuatro años de prisión.
>
> Igual sanción se aplicará a quien obtenga o difunda una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con el fin de cometer delito.
>
> *El resaltado es nuestro.

El artículo 292-A que se pretende adicionar al Código Penal a través del artículo 12 del Proyecto de Ley 61 de 2024, busca criminalizar la creación, distribución y comercialización de programas informáticos maliciosos, para combatir la economía criminal que surge de su uso en delitos informáticos. La redacción actual del presente artículo combina dos elementos clave: el conocimiento de la finalidad del software "*a sabiendas de su finalidad*" y su naturaleza "*concebido o adaptado para la comisión de delitos*". Esta combinación de elementos podría producir una interpretación problemática donde la simple posesión de un dispositivo de esta clase, incluso con fines legítimos, constituiría un delito.

Aunado a ello, las condiciones planteadas en el artículo 12 del Proyecto de Ley crean un riesgo legal particular para los profesionales de ciberseguridad. Expertos informan que en la práctica se realizan pruebas de vulnerabilidades y de penetración a sistemas informáticos para garantizar la ciberseguridad, el cual tiene la finalidad de verificar sistemas robustos como los sistemas bancarios y de infraestructuras calificadas como críticas.

En el medio tecnológico, como medidas preventivas ante la ciberdelincuencia, se han desarrollado programas en los que una empresa invita a hackers éticos a identificar vulnerabilidades en sus sistemas informáticos y ofrece recompensar a quienes encuentren fallos.

Por ejemplo, un analista forense que posea muestras de algún programa informático para su estudio y desarrollo de contramedidas, podría ser considerado como infractor de la ley, lo que podría conllevar a criminalizar inadvertidamente actividades profesionales legales y necesarias para la protección de sistemas informáticos.

En nuestra opinión, el artículo 12 del Proyecto de Ley 61 de 2024, es contrario a principios fundamentales contenidos en el Código Procesal Penal, precisamente en los artículos 8 y 14, a saber:

> **Artículo 8.** Inocencia. Toda persona debe ser tratada y considerada como inocente durante la investigación y el proceso, hasta tanto se declare responsable del delito que se le imputa en sentencia que haga tránsito a cosa juzgada.
>
> **Artículo 14.** Respeto a los derechos humanos. Las partes en el proceso penal serán tratadas con el respeto debido a la dignidad inherente al ser humano. Los derechos y las garantías que consagran la Constitución Política, los tratados y convenios internacionales de derechos humanos y este Código deben considerarse como mínimos, prevalentes y no excluyentes de otros

que incidan sobre los derechos fundamentales y la dignidad de la persona.

La inconveniencia del artículo 12 del Proyecto de Ley 61, recae en que para la implementación de un artículo como el 292-A, que preserve el espíritu de la iniciativa de ley, el cual es tipificar un delito informático, la redacción de este artículo debería mantener elementos subjetivos específicos dirigidos a demostrar la intención de cometer el delito, o bien, excepcionar en el tipo penal propuesto, las circunstancias éticas que justifican la posesión de estos programas informáticos con fines no delictivos.

Es importante mencionar que el Proyecto de Ley 61 surge de una propuesta de ley presentada por el Procurador General de la Nación, la cual fue fusionada en su etapa de formación con los Proyectos de Ley 45 y 50; y que, la composición inicial dada al artículo 292-A, era del tenor siguiente:

> **Artículo 11.** Se adiciona el artículo 292-A al Código Penal, así:
>
> **Artículo 292-A.** Quien produzca, venda, obtenga para su utilización, posea, importe, difunda o de cualquier otra forma ponga a disposición cualquier dispositivo, incluido un programa informático, concebido o adaptado para la comisión de delitos a los que se refiere el presente Capítulo, a sabiendas de su finalidad, será sancionado con dos a cuatro años de prisión.
>
> Igual sanción se aplicará a quien obtenga o difunda una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con el fin de cometer delito.
>
> **No se considera delito a la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el presente artículo que no tenga por objeto la comisión de uno de los delitos previstos en el Código Penal, ni tampoco la divulgación de datos informáticos o documentos indispensables para la compresión de la historia, las ciencias, las artes o cualquier información que sea de interés público.**
>
> *El resaltado es nuestro.

De la lectura del texto reproducido, podemos observar que la propuesta de ley presentada por el Procurador General de la Nación comprendía en el tercer párrafo una excepción o condición al valorar la comisión del delito, siendo esta que no se

consideraría como tal, cuando las acciones no tuviesen por objeto la comisión de uno de los delitos tipificados en el Código Penal.

La carencia de tal condicionante conlleva a que el artículo 12 del Proyecto de Ley 61, sea inconveniente por no presumir la inocencia de una persona, que, con fines lícitos pueda utilizar, poseer, importar o difunda un dispositivo, incluido un programa informático, que pueda considerarse malicioso.

B. De la objeción parcial, por inexequible

1. Se objeta parcialmente, por inexequible, el artículo 12 del Proyecto de Ley 61 de 2024, por contravenir lo dispuesto en el artículo 22 de la Constitución Política de la República:

> **Artículo 22.** Toda persona detenida debe ser informada inmediatamente y en forma que le sea comprensible, de las razones de su detención y de sus derechos constitucionales y legales correspondientes.
>
> **Las personas acusadas de haber cometido un delito tienen derecho a que se presuma su inocencia** mientras no se pruebe su culpabilidad en juicio público que le haya asegurado todas las garantías establecidas para su defensa. Quien sea detenido tendrá derecho, desde ese momento, a la asistencia de un abogado en las diligencias policiales y judiciales.
>
> La Ley reglamentará esta materia.
>
> *El texto resaltado es nuestro

El artículo 12 del Proyecto de Ley 61 de 2024 posee elementos que vulneran el principio de presunción de inocencia consagrado en el citado artículo 22 de la norma constitucional, ya que como hemos expresado en líneas anteriores, la redacción dada al artículo 12 no contempla la posibilidad que una persona, pueda utilizar herramientas (programas informáticos) que puedan ser adaptadas para uso delictivos, con fines lícitos como, por ejemplo, propósitos investigativos, educativos o de estudio.

En consecuencia, el artículo 12 del Proyecto de Ley 61 de 2004, resulta inconstitucional ya que podría criminalizar inadvertidamente actividades profesionales legítimas y necesarias para la protección de sistemas informáticos.

2. Se objeta parcialmente, por inexequible, el artículo 16 del Proyecto de Ley 61 de 2024, por contravenir lo dispuesto en el artículo 32 de la Constitución Política de la República:

> **Artículo 32.** Nadie será juzgado, sino por autoridad competente y conforme a los trámites legales, y no más de una vez por la misma causa penal, administrativa, policiva o disciplinaria.

El artículo 16 del Proyecto de Ley 61 de 2024, lee así:

> **Artículo 16.** Se adiciona el Capítulo VI, contentivo de los artículos 338-A, 338-B, y 338-C y 338-D, al Título I del Libro Tercero del Código Procesal Penal, así:
>
> **Capítulo VI**
> Evidencia Digital
>
> **Artículo 338-A**. ...
>
> ...
>
> **Artículo 338-C**. Orden de Suministro. El Ministerio Público podrá ordenar a una persona natural o jurídica que suministre datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático, o a un proveedor que ofrezca sus servicios en el territorio nacional, que suministre los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.
>
> **Cuando Ministerio Público logre la obtención de los datos correspondientes los someterá al control posterior del Juez de Garantías, de conformidad con las reglas establecidas en este Código para la incautación de datos.**
>
> ...
>
> *El texto resaltado es nuestro.

Como podemos observar, el artículo 16 del Proyecto de Ley 61 de 2024 que introduce, entre otros, el artículo 338-C al Título I del Libro Tercero del Código Procesal Penal, otorga al Ministerio Público el poder de ordenar a una persona natural o jurídica suministrar datos informáticos, sin tomar en cuenta lo que el Código Procesal Penal dispone respecto a los actos de investigación que requieren autorización de juez de garantías, en el Capítulo II del Título I del Libro Tercero, veamos:

Artículo 296. Autorización judicial. El Ministerio Público deberá requerir, por escrito a través de cualquier medio idóneo, la autorización para el allanamiento debidamente fundado, que deberá contener:

1. ...

Artículo 297. Autorización del allanamiento. El Juez examinará el cumplimiento de los requisitos formales y la razonabilidad de los motivos de la solicitud del Fiscal. La petición deberá ser resuelta inmediatamente y sin más trámites y no podrá exceder de dos horas desde que fue recibida por el Juez de Garantías, quien hará constar la autorización en el mismo escrito, indicando el término para iniciar la diligencia.

El Juez conservará una copia y otra será entregada, en el momento del allanamiento, al titular, al encargado o a quien se encuentre en el domicilio o, en su defecto, a un vecino.

Artículo 298. Excepciones. Cuando sea necesario, para evitar la comisión de un delito o en respuesta a un pedido de auxilio para socorrer a víctimas de crímenes o desastres o en caso de flagrancia, podrá procederse al allanamiento sin autorización judicial.

De igual modo, el Fiscal podrá ordenar la realización del allanamiento si hay peligro de pérdida de la evidencia o si se deriva de un allanamiento inmediatamente anterior. En estos casos, la diligencia deberá ser sometida al control del Juez de Garantías, en la forma prevista en el artículo 306 de este Código.

Artículo 299. Límites. Todo allanamiento se limitará exclusivamente a la ejecución del hecho que lo motiva y no se extenderá a otros hechos no señalados.

Al colocar el control correspondiente del juez de garantía posterior a la adquisición de datos informáticos por parte del Ministerio Publico, podemos observar que existe una inconstitucionalidad por violación al principio del debido proceso, consagrado en el artículo 32 de la Constitución Política, el cual, como derecho fundamental, además de garantizar un proceso justo, busca la correcta aplicación de las leyes.

Como podemos leer, de los artículos 296, 297, 298, y 299 del Código Procesal Penal, el Ministerio Público debe requerir al Juez la autorización para un allanamiento, quien posteriormente examinará el cumplimiento de los requisitos formales y la razonabilidad de los motivos de la solicitud del Fiscal. En ese sentido, la ley establece excepciones para el allanamiento sin autorización judicial, para situaciones especiales.

Si bien, el mencionado artículo 16 busca otorgar una herramienta investigativa ágil para la obtención de datos informáticos, con la finalidad de evitar la pérdida de la evidencia digital, existe una omisión del debido proceso ya establecido en el Código Procesal Penal, para estos casos, razón por la cual el mismo es inconveniente e inexequible.

3. Conclusión.

El Proyecto de Ley 61 es una iniciativa significativa para fortalecer el marco jurídico panameño frente a los delitos cibernéticos. La constante evolución de la tecnología y las amenazas en el ámbito digital requieren instrumentos legales actualizados que permitan una respuesta efectiva del sistema judicial. No obstante, el análisis realizado muestra deficiencias significativas en la sintaxis legal de artículos clave, como el uso de términos excesivamente amplios, y condicionantes que podrían resultar en la criminalización de actividades legítimas.

Aunque reconocemos la urgente importancia de actualizar la legislación en materia de ciberdelincuencia, es imperativo que sea conforme a la Constitución Política de la República, los tratados internacionales y los derechos humanos fundamentales.

Considero parcialmente inconveniente e inexequible el contenido de la propuesta de Ley, ya que, como he expresado, algunas de las disposiciones planteadas en el Proyecto de Ley vulneran derechos fundamentales como lo son el debido proceso, y la presunción de inocencia, consagrados en la Constitución y en la ley.

En virtud de las consideraciones previamente expresadas y en ejercicio de las facultades que me confiere el artículo 169 y el numeral 6 del artículo 183 de la Constitución Política de la República, considero necesario devolver a esa Asamblea Nacional, sin haber sido objeto de la sanción correspondiente, el Proyecto de Ley 61 de 2024, **Que modifica y adiciona artículos al Código Penal, al Código Procesal Penal y a la Ley 11 de 2015, sobre asistencia jurídica internacional en materia penal, y dicta otra disposición, respecto a medidas contra la ciberdelincuencia** con la finalidad de que esa augusta cámara proceda a la consideración y análisis de estas objeciones.

Reciba honorable diputada presidenta, las muestras de mi consideración y estima.

Atentamente,

JOSÉ RAÚL MULINO QUINTERO
Presidente de la República