



“2024 - Año de la digitalización y simplificación administrativa, de las startups, de la inteligencia artificial, del desarrollo de la ciudadanía digital y de la salud mental”.

PROYECTO DE LEY
LA CÁMARA DE REPRESENTANTES DE LA PROVINCIA
SANCIONA CON FUERZA DE
LEY

ARTÍCULO 1.- Se sustituye el artículo 214 del Título II- Disposiciones Generales Para la Investigación Formal de la Ley XIV N. ° 13 - Código Procesal Penal de la Provincia de Misiones, el que queda redactado de la siguiente manera:

“ARTÍCULO 214.- Libertad y Legalidad probatoria. Todos los hechos y circunstancias relacionadas con el objeto del proceso pueden ser acreditados por cualquier medio de prueba. No regirán respecto de ellos las limitaciones establecidas por las leyes civiles, con excepción de las relativas al estado civil de las personas.

Además de los medios de prueba establecidos, se podrán utilizar otros siempre que no vulneren garantías constitucionales de las personas o afecten el sistema institucional. Las formas de admisión y producción se adecuarán a los medios de prueba previstos en este Código.

Los elementos de prueba tendrán valor si han sido obtenidos por un medio lícito e incorporados al procedimiento conforme a las disposiciones de este Código”.

ARTÍCULO 2.- Se incorpora el Capítulo IX- METODOLOGÍAS PARA LA OBTENCIÓN DE EVIDENCIA DIGITAL, el que se conforma por los artículos 283 bis, 283 ter, 283 quáter y 283 quinquies al Título III - Medios de Prueba, del Libro II – Instrucción, de la Ley XIV - N. ° 13 Código Procesal Penal de la Provincia de Misiones, el que queda redactado de la siguiente manera:

“CAPÍTULO IX
METODOLOGÍAS PARA LA OBTENCIÓN DE EVIDENCIA DIGITAL

ARTÍCULO 283 bis.- Metodologías para la obtención de evidencias digitales, informáticas, electrónicas y de tráfico. El Juez, mediante auto fundado y motivado, puede ordenar la obtención de evidencias indispensables para la investigación preliminar. La medida debe estar debidamente motivada, especificando el ámbito, objeto, alcance y duración.

Cod_Ver:250286



Si existe sospecha de que los datos y evidencias digitales obtenidas pueden ser susceptibles de pérdida o modificación y están almacenados en diferentes soportes y dispositivos, puede ordenar su aseguramiento, conservación y registro, incluyendo a los datos de tráfico de comunicaciones específicas.

El proveedor del servicio de comunicación e internet requerido debe informar inmediatamente al Juez si en la transmisión participaron uno o más prestadores del servicio, con la finalidad de identificarlos y asegurar los datos de tráfico de la comunicación, a fin de que presenten, remitan o entreguen toda la información relacionada a los usuarios del servicio, en el marco de la investigación.

A los efectos de proceder con estas metodologías, el Juez podrá:

1. Ordenar por decreto fundado el secreto de las medidas de aseguramiento y conservación de todo el actuado a las partes involucradas, conforme lo dispone el artículo 212;
2. Autorizar la realización de operaciones técnicas de constatación necesarias para determinar cuáles son los dispositivos, sistemas y archivos que contienen los datos y evidencias que motivan la medida, ordenando la obtención y retención inmediata de los datos y soportes donde se encuentren almacenadas las evidencias digitales;
3. Requerir que durante el cumplimiento de la medida, esta se realice mediante acceso en tiempo real cuando exista riesgo de alteración o pérdida y los datos y evidencias estén contenidos en memorias volátiles;
4. solicitar la colaboración de expertos en seguridad informática, así como de las empresas prestatarias de los servicios de comunicaciones e internet, no pudiendo extenderse a personas que deben o pueden abstenerse de declarar como testigos por razón de parentesco, secreto profesional o de Estado.

ARTÍCULO 283 ter.- Metodologías para la obtención remota de evidencias digitales, informáticas, electrónicas y de tráfico. El Juez puede ordenar mediante auto fundado la obtención de evidencias y datos de manera remota, a través del uso de programas y herramientas informáticas forenses y otros mecanismos tecnológicos, siempre que existan motivos suficientes que acrediten la imposibilidad de ser obtenidos de otra manera.

La medida que ordene la obtención de evidencias y datos de manera remota debe detallar los datos personales de los funcionarios encargados de la ejecución, el tiempo de la intervención y su prórroga por igual período si se mantienen los motivos que fundamentaron la medida. Alcanzados los objetivos que motivaron la intervención remota, el Juez debe ordenar su cese, asegurando que se descarten de los soportes y dispositivos todos los programas y herramientas informáticas forenses autorizadas.

Las evidencias y datos obtenidos podrán ser incorporados al proceso, siempre que la metodología de obtención se ajuste estrictamente a lo ordenado en la medida. Si durante la ejecución de la medida los funcionarios tienen razones suficientes para sospechar que



"2024 - Año de la digitalización y simplificación administrativa, de las startups, de la inteligencia artificial, del desarrollo de la ciudadanía digital y de la salud mental".

los datos y evidencias se encuentran en otros soportes, dispositivos y sistemas, deben poner en conocimiento inmediatamente al Juez, quien podrá autorizar la ampliación de los términos de la orden, y de ello se debe notificar de inmediato al Fiscal.

Ordenada la medida, el Juez debe poner en conocimiento de la misma al titular del objeto de la orden que autorizó el acceso remoto, al imputado y su defensor. El órgano responsable de la ejecución es la Secretaría de Apoyo para las Investigaciones Complejas, dependiente del Cuerpo de Investigaciones Complejas del Superior Tribunal de Justicia de Misiones, a través de su personal técnico idóneo.

En todos los casos, el Juez debe fundamentar la idoneidad, necesidad y proporcionalidad de las medidas y correr vista al Fiscal, todo bajo pena de nulidad. Asimismo, debe garantizar mediante medios tecnológicos adecuados que las evidencias y datos digitales sean auditables, a los fines de asegurar la cadena de custodia y control, conforme lo dispone el artículo 208 del Título II - Disposiciones Generales para la Investigación Formal.

Estos supuestos se regirán, en cuanto sean aplicables, por lo previsto en los artículos 232, 233, 234, 235, 236, 237, 238 y 239, garantizando a través de medios físicos y técnicos la inalterabilidad de los datos contenidos en los soportes y dispositivos secuestrados.

Artículo 283 quater.- Hallazgo casual: procede cuando en el marco del cumplimiento de una orden de las descriptas en este capítulo surge por:

1. descubrimiento: Durante la ejecución de una orden de obtención o registro, si se descubren evidencias relacionados con un posible delito diferente al que motivó la medida, los funcionarios deben informar de inmediato al Juez y al Fiscal.

La ampliación de la orden debe realizarse bajo pena de nulidad.

2. extensión a otros soportes, dispositivos o sistemas: Si existe sospecha suficiente que las evidencias y los datos pueden hallarse o se encuentran almacenados en otros soportes, dispositivos o sistemas, la medida puede extenderse a ese otro sistema. Es necesario notificar al juez y al fiscal para obtener la ampliación de autorización correspondiente.

3. Jurisdicción Extranjera: si al ejecutarse la medida emerge que las evidencias digitales y los datos están almacenados en una jurisdicción extranjera la orden puede ampliarse cuando:

a. la persona poseedora de los soportes, dispositivos o el titular usuario de un sistema objeto de la orden concede voluntariamente su revelación;

b. sin ejercer actos de poder jurisdiccional, es posible acceder a los datos y evidencias desde el sistema principal;

En casos de incertidumbre, la medida debe ordenarse para realizar copias de las

Cod_Ver:250286



evidencias y de los datos relevantes para la investigación.

Cuando así lo considere, el juez puede encomendar su cumplimiento por medio de exhorto a la jurisdicción correspondiente, conforme lo establece el artículo 140 del Capítulo III- Suplicatorias, Exhortos, Mandamientos y Oficios, del Título V- Actos Procesales, a los efectos de la obtención de los datos requeridos para la investigación.

ARTÍCULO 283 quinquies.- Investigación en incógnito. Perfil digital encubierto. En casos relacionados a delitos complejos, en que resulte indispensable la intervención en incógnito de un agente a través de los canales cerrados de comunicación, entornos y plataformas digitales, el Juez puede ordenar la intervención en incógnito de un agente mediante la autorización del uso de un perfil encubierto.

Esta metodología es de carácter excepcional y debe emitirse por auto fundado siempre que el éxito de la investigación se encuentre entorpecido y se trata de delitos cometidos a través de medios informáticos que no admitan otra forma de investigación.

La actuación de un agente mediante el perfil encubierto debe autorizarse estableciendo la modalidad, la duración y en su caso, de ser necesaria la prórroga si se mantienen los motivos que fundamentó de la medida.

El juez debe controlar periódicamente los perfiles o identidades digitales que serán creados y administrados por personal técnico idóneo de la Secretaría de Apoyo para la Investigaciones Complejas dependiente del Cuerpo de Investigaciones Complejas del Superior Tribunal de Justicia.

Además, se hará constar las directivas, reservando y asegurando en soportes y dispositivos digitales, la denominación, características del perfil utilizado por el agente encubierto, los canales de comunicación en los que intervendrá, las plataformas digitales donde actuará, las claves de acceso validadas y la actuación concreta a desempeñar.

Concluida la intervención del agente encubierto, el Juez debe dejar constancia de la existencia en el legajo judicial.

El agente encubierto autorizado por auto fundado, podrá intercambiar o enviar archivos de contenido prohibido o ilegales con la finalidad de: identificar o detener a los autores, partícipes o encubridores, impedir la consumación de un delito o para reunir información, datos, evidencias digitales o elementos de prueba necesarios para la investigación.

En estos supuestos y con los recaudos establecidos en los párrafos anteriores, la actuación del agente encubierto no constituye delito.

Se considera agente encubierto al funcionario o miembro autorizado de la Secretaría de Apoyo para la Investigaciones Complejas dependientes del Cuerpo de Investigaciones Complejas del Superior Tribunal de Justicia de Misiones, que previo prestar su consentimiento, oculte o utilice un perfil digital encubierto, interactúe y se relacione a través de tecnologías de la información y de la comunicación”.



"2024 - Año de la digitalización y simplificación administrativa, de las startups, de la inteligencia artificial, del desarrollo de la ciudadanía digital y de la salud mental".

ARTÍCULO 3.- Comuníquese al Poder Ejecutivo.

FUNDAMENTOS:

El presente proyecto de ley pretende modificar el Código Procesal Penal de la Provincia de Misiones (Ley XIV-Nº 13), sustituyendo el artículo 214 e incorporando un capítulo denominado "Metodologías para la obtención de evidencia digital". Estas herramientas son novedosas, útiles y necesarias para el servicio de justicia. La denominada cuarta revolución industrial, en tanto proceso global de convergencia de tecnologías digitales, físicas y biológicas emergentes, y la digitalización, implica profundas transformaciones en la manera en que se relacionan los seres humanos entre sí y con el entorno. Ello ha derivado en la multiplicación de la transmisión de la información en formato digital, utilizada frecuentemente en la vida cotidiana debido al auge de Internet. La red de redes permite interactuar de variadas formas para socializar, comprar, vender, viajar, esparcirse, entre otros múltiples y legítimos motivos.

Es así que han crecido de manera exponencial las interacciones e intercambios de datos en aplicaciones de mensajería, redes sociales, correos electrónicos, internet 4.0, internet de las cosas, análisis de datos, computación en la nube y automatización de procesos, entre otros. Estas interacciones se han denominado "personalidad digital". Todo ello deriva en la existencia de nuevos entornos de desarrollo de la personalidad que deben ser protegidos ante el aumento exponencial de los riesgos. Estos riesgos muchas veces involucran la realización de actividades criminales, a expensas de ciudadanos digitales, quienes no son aún conscientes de las nuevas amenazas que presenta la virtualidad. Así, se reiteran hechos de estafas digitales, amenazas virtuales aprovechando el "anonimato" de la red, secuestros virtuales, entre otras lesiones o riesgos para bienes jurídicos.

Estos nuevos riesgos a veces se despliegan de manera dramática, agravando la vulnerabilidad de sectores ya de por sí sensibles de nuestra población, como los niños, niñas y adolescentes. La ley de fondo ha establecido nuevas conductas típicas para alcanzar estas formas de criminalidad en la red, como la pornografía infantil y el grooming, que victimizan a nuestras infancias. A este nuevo entramado se incorpora la utilización de inteligencia artificial generativa, capaz de desarrollar texto, imagen y



video de manera interoperable, creando productos a veces indistinguibles de los objetos de la realidad física. Se evidencia entonces el traslado de la vida de las sociedades a entornos virtuales e internet, incrementándose también la criminalidad en dichos ámbitos, en algunos casos organizada en redes de complejo análisis y desarticulación. Básicamente, la vida en la moderna sociedad de la información y la comunicación da lugar a nuevos entornos que deben ser resguardados de nuevos riesgos.

De allí la necesidad de incrementar y validar las herramientas tecnológicas para su utilización por parte del servicio de Justicia, incorporándolas a los procesos judiciales, en particular el proceso penal, resguardando al mismo tiempo los derechos y garantías constitucionales. La revolución tecnológica y digital ha transformado la forma en que se cometen los delitos, se recopilan pruebas y se llevan a cabo las investigaciones penales. Como resultado, es necesario actualizar nuestro sistema legal para garantizar que esté a la altura de los desafíos y oportunidades que presenta esta nueva era. El proyecto de ley propuesto tiene como objetivo principal proporcionar un marco normativo claro y actualizado para la utilización de herramientas digitales como medios de prueba en el proceso penal de la Provincia de Misiones. La incorporación de estas disposiciones legales permitirá fortalecer la eficacia y la transparencia del sistema de justicia penal, al tiempo que se protegen los derechos fundamentales de los ciudadanos.

La Convención de Budapest sobre Ciberdelincuencia, aprobada por Ley Nacional N° 24.711, es el primer tratado internacional que aborda el delito cibernético y la seguridad cibernética de manera integral. Fue adoptada en 2001 por el Consejo de Europa y ha sido ratificada por numerosos países, estableciendo un marco legal para la lucha contra los delitos informáticos y la protección de los datos en línea. Los principios y herramientas de la Convención de Budapest son relevantes para el presente proyecto de ley sobre herramientas digitales como medios de prueba en el proceso penal de la Provincia de Misiones, ya que proporciona directrices y estándares internacionales en áreas clave relacionadas con la obtención y el manejo de evidencia digital. Los artículos 16 a 21 de la Convención de Budapest establecen el orden de intervención progresiva y secuenciada sobre la información y, por lo tanto, los datos e información del imputado, a saber: la conservación rápida de los datos almacenados, la conservación y revelación parcial de los datos relativos al tráfico, las órdenes de presentación de datos, el registro y confiscación de los datos, la obtención en tiempo real de datos relativos al tráfico y, finalmente, la interceptación de datos relativos al contenido. Estos principios encuentran su reflejo en cada una de las herramientas trazadas en el proyecto adjunto.

Estos principios se han reconocido como “la regla de los tres escalones” (Dupuy y Kiefer, 2018). Esta hace referencia a tareas de investigación que se ejecutan en el marco de una causa penal, ordenándolas según el nivel de intensidad en que comprometen o puedan comprometer garantías constitucionales. La base de la pirámide escalonada estaría comprendida y apuntalada sobre la incorporación al proceso penal de los datos públicos, a los cuales se puede acceder de forma irrestricta y sin vulnerar



"2024 - Año de la digitalización y simplificación administrativa, de las startups, de la inteligencia artificial, del desarrollo de la ciudadanía digital y de la salud mental".

ninguna "barrera técnica o jurídica". Ejemplifica tales actos con la búsqueda, identificación y procesamiento de información sobre fuentes abiertas, que pueden obtenerse de forma pública. Luego, el primer escalón de la pirámide estaría comprendido por los datos de abonado, identificación de usuario, o la información básica del suscriptor en el caso de las redes sociales. Sobre este primer peldaño, el autor considera que los datos identificatorios son personales y avanzan sobre una primera barrera de privacidad de la persona investigada. Por otra parte, el segundo grado de la regla estaría dado por los datos de tráfico, es decir, los datos de origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente. Finalmente, el tercer y último nivel estaría comprendido por los datos de contenido. Este sería, según el autor, el nivel máximo de compromiso de garantías por cuanto implica el conocimiento del contenido mismo de la comunicación.

De allí que resulte fundamental sustentar las medidas dispuestas por el Juez sobre determinados principios generales, los cuales emergen de la literatura y jurisprudencia comparada bajo la forma del principio de razonabilidad y sus subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto. El subprincipio de idoneidad o adecuación establece que la normativa debe ser idónea para lograr el fin perseguido por el legislador. Es decir, debe ser capaz de alcanzar ese objetivo de manera efectiva. Posteriormente, el subprincipio de necesidad demanda que se seleccione el medio menos restrictivo de derechos individuales posible entre aquellos que son idóneos para alcanzar el fin buscado. Esto implica un análisis comparativo entre diferentes opciones para determinar cuál es la menos invasiva de los derechos fundamentales en juego.

Una vez cumplidos los requisitos de adecuación y necesidad, se debe evaluar si la normativa es razonable estrictamente hablando. Esta evaluación consiste en determinar si existe una relación equilibrada entre los beneficios que se obtienen con la medida y los posibles perjuicios que pueda generar sobre otros bienes o valores en conflicto. En otras palabras, se busca garantizar que los beneficios superen a las desventajas de manera proporcionada. En particular, respecto al texto propuesto, el proyecto de ley propuesto busca reformar el Código Procesal Penal de la Provincia de Misiones, específicamente introduciendo y modificando artículos clave para mejorar la obtención y manejo de evidencias digitales. En primer lugar, el proyecto sustituye el artículo 214, estableciendo la libertad y legalidad probatoria, permitiendo que todos los hechos y circunstancias relacionadas con el objeto del proceso puedan ser acreditados por cualquier medio de prueba, siempre que no se vulneren garantías constitucionales ni se afecte el sistema institucional. Esta modificación asegura una mayor flexibilidad y eficacia en la presentación de pruebas durante el proceso judicial.

Además, se incorpora un nuevo Capítulo IX, titulado "Metodologías para la

Cod_Ver1:250286



Obtención de Evidencia Digital", que introduce los artículos 283 bis, 283 ter, 283 quáter y 283 quinquies. Estos artículos detallan las metodologías para la obtención de evidencias digitales, informáticas, electrónicas y de tráfico, incluyendo procedimientos remotos y el uso de perfiles digitales encubiertos en investigaciones complejas. Se establece que el juez, mediante auto fundado, puede ordenar la obtención de evidencias digitales indispensables para la investigación, especificando los procedimientos y salvaguardas necesarias para asegurar la integridad y legalidad de las pruebas obtenidas. Finalmente, el proyecto contempla la posibilidad de hallazgos casuales y la extensión de la jurisdicción en la obtención de pruebas digitales. Se regula la ampliación de órdenes cuando surgen nuevas evidencias durante una investigación y se permite la cooperación internacional en casos donde las evidencias digitales se encuentren en jurisdicciones extranjeras. La inclusión del artículo 283 quinquies permite la intervención encubierta de agentes en investigaciones de delitos complejos a través de perfiles digitales, asegurando que estas acciones se realicen bajo estrictas condiciones de legalidad y control judicial. Este proyecto de ley fortalece el marco legal para la investigación de delitos en el ámbito digital, respondiendo a las necesidades contemporáneas de justicia y seguridad.

Este enfoque garantiza que las medidas legislativas respeten los derechos fundamentales, equilibrando la protección de esos derechos con la consecución de los objetivos perseguidos por la ley. En última instancia, se busca asegurar la prevalencia de los derechos de mayor valor frente a la problemática específica que motiva su invocación y aplicación. Al momento del dictado del auto fundado, el juez deberá hacer el adecuado balance y ponderación de bienes en juego, los objetivos perseguidos y los derechos involucrados, para otorgar la máxima satisfacción posible a las necesidades de la justicia, con el menor compromiso o restricción de los derechos fundamentales de aquellos afectados por dichas medidas. En este sentido, es que proponemos las modificaciones en el Código Procesal Penal de la provincia de Misiones, así como la adición de una serie de artículos que regulen aspectos específicos relacionados con la obtención y utilización de datos informáticos y electrónicos como medios de prueba en procesos penales.

Este proyecto de ley tiene como finalidad adaptar nuestro sistema judicial a los desafíos y oportunidades que presenta el avance tecnológico, permitiendo un adecuado resguardo frente a los riesgos de la Cuarta Revolución Industrial, al mismo tiempo que garantiza el respeto de los derechos fundamentales mediante intervenciones basadas en el principio de razonabilidad y sus subprincipios de idoneidad, necesidad y proporcionalidad. Por todo ello, solicito a mis pares la aprobación del presente proyecto de ley.