HONORABLE
LEGISLATURA
DE LA PROVINCIA
DEL CHUBUT

CHUBUT

L E Y XV Nº 43 .

LA LEGISLATURA DE LA PROVINCIA DEL CHUBUT

SANCIONA CON FUERZA DE

L E Y

Investigación, prevención y lucha contra los delitos complejos y la cibercriminalidad. Regulación de la Evidencia Digital y de las herramientas informáticas aplicadas a la investigación penal, Agente Encubierto Digital y el Acceso remoto a dispositivos electrónicos.

CAPITULO 1

DISPOSICIONES GENERALES.

Artículo 1°. Medios de prueba informáticos. Principios generales. La realización de cualquiera de las medidas o la utilización de las herramientas previstas en esta ley deberá ser dispuesta, ordenada o autorizada, siempre en el marco de una investigación penal concreta, definiendo detalladamente el ámbito objetivo y subjetivo, la duración de la medida en virtud de su utilidad para la investigación y consignándose el dato o información concreta a relevar u obtener.

En el uso de estos medios de prueba se procurará siempre la menor afectación posible a los derechos de las personas investigadas o terceros afectados conforme a las necesidades de la investigación. La resolución que la disponga o autorice deberá fundamentar la idoneidad, necesidad y proporcionalidad de la medida de conformidad a lo previsto en el artículo 25 del C.P.P.Ch. (art. 169 I, C.Ch.).

Toda medida a realizar o realizada, así como la información recolectada por ella en el marco de la investigación, debe permanecer en secreto, con obligación de no divulgación para todas las partes del proceso, hasta el acto propio de la audiencia oral, pública y contradictoria. Toda divulgación indebida o utilizada con fines de estigmatización o que genere un perjuicio indebido será considerada falta grave

Artículo 2°. Evidencia Digital. Definición. Principios Generales. Se entiende por evidencia digital todo dato, información o conjunto de datos generados, almacenados, transmitidos o procesados mediante tecnologías digitales, electrónicas o informáticas, incluyendo dispositivos físicos, sistemas informáticos, redes, servicios en la nube, plataformas digitales y entornos virtuales, que obtenidos y documentados conforme a las reglas legales y técnicas vigentes, resulte auténtico, íntegro, trazable y verificable, y posea aptitud para acreditar o refutar hechos relevantes en un proceso penal.

Cuando en el ejercicio de su función los representantes del MPF tomen conocimiento de la existencia de evidencia digital relacionada con el o los hechos sujetos a investigación, o con las personas sindicadas como autores o partícipes, deberán adoptar todas las medidas necesarias y adecuadas para proceder a su correcta individualización, identificación, recolección, preservación, procesamiento y presentación, conforme las normas y protocolos vigentes o que se dispongan en cada caso.

Artículo 3°. Aseguramiento de datos. De conformidad con lo previsto en el artículo 112 del CPPCh y el artículo 6 de la Ley VN°94, el fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema informático o en un dispositivo de almacenamiento informático que esté bajo su disposición o control y para el que tenga legítimo acceso, cuando los datos puedan ser de utilidad en una investigación concreta y tenga motivos para sospechar que éstos pueden ser alterados o suprimidos o de cualquier forma dejar de estar disponibles.

La orden deberá especificar los datos que se pretenden asegurar, la modalidad técnica de la conservación y la duración de la medida que no podrá exceder de noventa (90) días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden.

El requerido deberá arbitrar los medios necesarios para preservar de inmediato la integridad de los datos en cuestión y, cuando así le sea ordenado, deberá mantener bajo secreto la medida de aseguramiento.

Las personas involucradas en el cumplimiento de la orden deberán guardar reserva y abstenerse de informar sobre ellas en los términos del artículo 257 del Código Procesal Penal del Chubut.

Cuando el objeto de la medida prevista en los párrafos anteriores sea el aseguramiento de datos de tráfico relativos a una determinada comunicación, el proveedor de servicio requerido, informará al fiscal -lo antes posible- si hubiera otros proveedores de servicio por medio de los cuales aquella comunicación haya sido efectuada, con el fin de identificar a todos los proveedores de servicio intervinientes en la comunicación y que, de esa manera, se puedan arbitrar las medidas necesarias para asegurar los datos del tráfico de la comunicación.

Artículo 4°. Orden de presentación de datos informáticos. El Fiscal podrá ordenar a organismos públicos y a personas humanas o jurídicas con sede en la Provincia, la presentación, remisión o entrega de datos informáticos que se encuentren bajo su poder o control y a los que puedan acceder de manera legítima, cuando se trate de datos de abonado o datos de identificación del usuario o del servicio.

Cuando el requerimiento comprenda datos de tráfico o de contenido, o cualquier otra información sujeta a secreto o protegida por una expectativa razonable de privacidad, el Fiscal deberá contar con autorización judicial previa.

Asimismo, el Fiscal podrá requerir a personas humanas o jurídicas con asiento fuera de la Provincia que presten servicios en ella, o a proveedores de servicios de internet o de comunicaciones que allí operen, la presentación de los datos comprendidos en los párrafos anteriores, en el marco de los convenios vigentes o mecanismos de cooperación aplicables.

43 La orden o requerimiento podrá disponer el secreto de la medida. Las personas involucradas deberán guardar reserva y abstenerse de informar sobre ella en los términos del artículo 257 del Código Procesal Penal del Chubut.

Artículo 5°. Requerimientos de los representantes del MPF. Los magistrados del Ministerio Público Fiscal, legalmente autorizados, podrán requerir, conforme los convenios vigentes o mecanismos de cooperación aplicables; cuando resulte necesario para identificar o localizar a una persona, información de abonado y de conexión a cualquier empresa nacional o internacional, que resulten prestadoras de servicios de telecomunicaciones, de internet o digitales, de servicios o medios de pago, del sistema financiero, de servicios electrónicos o cualquier otro servicio digital, en relación con la fecha del o los hechos investigados y por un plazo que no exceda de quince días.

Para requerir información de conexión o de tráfico por plazos superiores o en combinación con más de tres empresas en relación con la misma persona o grupo de personas, deberá contar con autorización judicial previa.

Artículo 6°. Medidas de investigación en fuentes abiertas. Los Fiscales podrán disponer u autorizar la realización de investigación en fuentes abiertas, debiendo entenderse por tal, aquellas a las que puede accederse de manera lícita sin superar barreras técnicas de acceso y sin vulnerar restricciones jurídicas de confidencialidad o secreto. Si de la investigación de fuentes abiertas surgieren datos que por su naturaleza deban ser protegidos, no podrán ser utilizados en ninguna investigación y deberán ser eliminados.

Artículo 7°. Otras Medidas. Los Fiscales podrán disponer, además:

a) En el caso de delitos económicos o que impliquen la transmisión de activos por medios digitales y cuando resulte indispensable para impedir la consumación de los efectos del delito, la pérdida de activos o la pérdida de evidencia digital; el bloqueo provisorio de canales digitales y/o la inmovilización de cuentas, fondos o sistemas, dando inmediata intervención judicial para su control.

b) cuando mediare urgencia, remover o secuestrar (preservar) los datos haciéndolos inaccesibles para terceros ajenos a las autoridades a cargo de la investigación utilizando para ello las medidas técnicas o herramientas informáticas que resulten adecuadas, dando inmediato aviso al Juez Penal para su debido contralor posterior.

c) cuando exista urgencia para obtener datos determinados a fin de evitar la concreción de un peligro inmediato para la vida o integridad física de las personas, o para impedir la consumación de los efectos de un delito de especial gravedad, o la pérdida irrecuperable de activos o evidencias digitales, podrá disponer del uso de la fuerza física indispensable para proceder al desbloqueo de los dispositivos electrónicos que posean patrón de huella dactilar o cualquier otro de tipo biométrico, disponiendo las medidas necesarias para asegurar el posterior acceso, inspección y aseguramiento de datos.

En los demás casos en que ello resulte necesario, deberá requerir la correspondiente autorización del Juez Penal, el que, verificados los extremos de los arts. 13, 18, 20, 34 y 183 del CPPCh, así podrá autorizarlo.

CAPITULO II

REGISTRO Y SECUESTRO DE SISTEMAS Y DATOS INFORMÁTICOS.

Artículo 8°. Obtención de datos informáticos. Registro y Secuestro.

1. Orden judicial. El Juez Penal podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de:

a) Secuestrar los componentes físicos del sistema y, si fuera necesario, los dispositivos para su lectura. En este supuesto regirán en cuanto sean aplicables, las previsiones del título II tomo I del Libro IV del CPPCh, procurando garantizar por medios físicos y técnicos la inalterabilidad de los datos contenidos en los soportes físicos secuestrados.

43

b) realizar copia en un soporte autónomo o en repositorio compartido de datos autorizado judicialmente, de todos los datos contenidos en los sistemas o dispositivos encontrados o de los datos que la orden judicial hubiera autorizado a secuestrar, garantizando por medios tecnológicos que los datos no puedan sufrir ningún tipo de modificación o alteración.

c) preservar por medios tecnológicos todos los datos contenidos en los dispositivos o aquellos datos identificados en la orden judicial asegurando que no puedan ser alterados o suprimidos.

d) remover o secuestrar los datos haciéndolos inaccesibles para terceros ajenos a las autoridades a cargo de la investigación.

A los fines de una ejecución más eficiente de la orden, especialmente cuando se encuentren en el lugar en el que se ejecuta la medida múltiples dispositivos o un importante volumen de datos que dificulte la ejecución, el Juez Penal, a pedido del fiscal, podrá autorizar que se realicen en el lugar las operaciones de constatación técnica necesarias para determinar qué dispositivos informáticos o archivos pueden contener datos alcanzados por la orden judicial, con la finalidad de limitar la cantidad de dispositivos o datos a registrar, copiar o secuestrar.

Estas operaciones técnicas también podrán ser autorizadas por el Juez Penal cuando exista urgencia para obtener datos determinados a fin de evitar la concreción de un peligro inmediato para la vida o integridad física de las personas.

Se deberá garantizar con los medios tecnológicos disponibles que resulten adecuados, que estas operaciones técnicas sean auditables, a los fines de garantizar la cadena de custodia y la posibilidad de control posterior de la medida por parte de la defensa.

El Juez Penal podrá autorizar que durante la ejecución de una orden de obtención de datos se acceda en vivo a datos contenidos en memorias volátiles, cuando exista riesgo de alteración o pérdida.

2. Hallazgos casuales. Cuando en el marco de un registro de dispositivos o sistemas informáticos o durante las tareas de peritaje, las autoridades que ejecutan la medida adviertan la presencia de datos vinculados a un posible hecho ilícito diferente, deberán comunicarlo de inmediato al juez penal.

Los datos así obtenidos solo tendrán validez siempre y cuando hayan sido encontrados de manera casual en cumplimiento y siguiendo los parámetros y requisitos establecidos en la orden judicial original.

3. Extensión de registros. En los supuestos en los que durante la ejecución de una medida de obtención de datos de un sistema informático surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema informático (servidor), al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla al otro sistema.

La ampliación del registro a los fines de la obtención o secuestro de datos deberá ser autorizada por el Juez Penal, quien fijará las condiciones de realización de la medida, salvo que esta situación estuviera prevista en la orden original.

Cuando sea posible determinar que los datos que son objeto de la medida se encuentren almacenados en extraña jurisdicción, la obtención de datos solo podrá ampliarse:

a) Si se cuenta con el consentimiento voluntario y lícito de la persona con facultades para disponer la revelación de los datos desde el dispositivo o sistema informático inicial.

b) cuando resulte posible recibir o acceder a los datos buscados desde el sistema original al que se accedió con la orden de obtención de datos, sin necesidad de realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en extraña jurisdicción.

c) cuando no resulte posible determinar en forma certera, al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados.

43 En los supuestos b) y c) se procurará restringir al máximo posible el alcance de la medida, copiando los datos que resulten de interés para la investigación y evitando la alteración, remoción o eliminación por cualquier forma de los datos a los que se accede.

La obtención de datos en extraña jurisdicción se notificará al Juez Penal que ordenó la extensión de registro, quien evaluará la necesidad o conveniencia de informar la medida y sus resultados a las autoridades de la jurisdicción correspondiente, de acuerdo con las normas de cooperación judicial vigentes.

4.- Cuando resulte necesario para la ejecución de la medida a pedido del fiscal, el Juez Penal podrá ordenar la colaboración de las empresas proveedoras de servicios de internet, de comunicaciones, o de terceras personas que tengan conocimientos especiales sobre las medidas de seguridad o el funcionamiento del sistema informático que es objeto de la medida. La orden no será aplicable a personas que puedan resultar imputadas o que estén alcanzadas por la dispensa de declarar como testigos por motivos de parentesco amistad estado.

Rigen en cuanto son aplicables todos los límites y garantías referidos al secuestro de cosas, documentos privados y correspondencia epistolar.

CAPITULO III

HERRAMIENTAS INFORMATICAS APLICADAS A LA INVESTIGACIÓN PENAL

Artículo 9°. Casos en los que pueden utilizarse. Las herramientas digitales de investigación podrán utilizarse en casos de delitos especialmente graves o cometidos por grupos organizados, entendiendo como tales a las asociaciones de tres o más personas que, mediante contacto personal o digital, realizan de forma reiterada o permanente conductas con el fin de cometer delitos. En estos casos el Fiscal podrá emplear o solicitar la autorización para utilizar las herramientas digitales detalladas en los artículos siguientes con el objetivo de investigar y obtener pruebas necesarias.

Artículo 10. Herramientas informáticas de investigación. El juez penal podrá autorizar, a requerimiento del representante del MPF, la adopción individual o conjunta de las medidas de investigación que se regulan en los artículos siguientes. La autorización estará supeditada a un examen de razonabilidad en el que el Juez deberá:

a) Comprobar que la medida a adoptarse esté relacionada con la investigación de un delito concreto y de especial gravedad.

b) evaluar la verosimilitud de la sospecha de que alguien, autor o partícipe, haya cometido, o intentado cometer, el delito objeto de la investigación.

c) descartar que no existan otras medidas menos gravosas para el investigado que resulten igualmente útiles para el esclarecimiento de los hechos o para averiguar el paradero de los imputados.

d) acreditar la existencia de una probabilidad suficientemente motivada de que una o varias de las medidas a adoptar proporcionarán elementos de prueba significativos para el avance de la investigación.

e) ponderar que el beneficio para el interés público que espera obtenerse guarde adecuada relación de proporcionalidad con la afectación de los derechos e intereses involucrados.

Artículo 11. Duración. Las medidas contempladas en el presente título tendrán la duración que para ellas se especifique en la orden que las autorice, la que no podrá exceder de tres (3) meses.

El Juez podrá renovar la medida, a pedido del Fiscal, siempre que subsistan las causas que la motivaron y previa exposición de los avances obtenidos hasta el momento. Transcurrido un (01) año, un tribunal de revisión (conforme art. 71 CPPCh.) deberá controlar los motivos que fundamenten que la medida continúe.

43 La medida de acceso remoto sobre equipos informáticos tendrá una duración máxima de un (1) mes, prorrogable hasta un máximo de tres (3) meses.

El Fiscal dispondrá el cese de las medidas autorizadas si desaparecieren las circunstancias que justificaron su adopción, o si resultare evidente que ellas no son idóneas para los fines pretendidos.

Artículo 12. Investigación encubierta en entornos digitales. Agente encubierto digital.

El Juez Penal, a requerimiento de las partes, podrá autorizar en el marco de una investigación concreta en el que se investigue la comisión de delitos señalados en el artículo 9 de la presente ley, la realización de investigaciones encubiertas en canales cerrados de comunicación, con el fin de identificar o detener a los autores, partícipes o encubridores, impedir la consumación de un delito, o para reunir elementos de prueba útiles para la investigación.

A tal fin, el Juez Penal podrá autorizar la designación de investigadores propuestos por el MPF para que actúen en forma encubierta. Podrán ser agentes encubiertos digitales los integrantes de las Fuerzas de Seguridad y del Cuerpo de Investigación Fiscal.

Los investigadores designados, podrán crear o utilizar perfiles o identidades digitales falsas poniendo en conocimiento al Fiscal a cargo de la investigación, quien deberá registrar toda la información

necesaria respecto a los perfiles o identidades falsas, sistemas informáticos en los que se utilizarán, claves de acceso validadas y actividad concreta a desarrollar.

El Juez Penal podrá autorizar que, durante la investigación encubierta, se intercambien archivos o contenidos ilícitos, se compren o vendan bienes, activos digitales o servicios, se participe de foros o grupos o cualquier actividad en entornos digitales con la finalidad de identificar a los responsables de los hechos ilícitos investigados.

En estos supuestos, no serán perseguibles quienes, como consecuencia necesaria del desarrollo de la investigación encubierta encomendada, hubieran cometido un hecho ilícito, siempre que guarden la debida proporcionalidad con la finalidad de la investigación y no implique poner en peligro cierto la

vida o la integridad psíquica o física de una persona o la imposición de un grave sufrimiento físico o moral a otro.

La medida será autorizada por el plazo estrictamente necesario para lograr la individualización de los autores, partícipes o encubridores, o para obtener y asegurar los medios de pruebas necesarios para su prosecución hasta por tres meses, prorrogables por igual plazo, siempre que el requerimiento se encuentre fundado en relación con la necesidad propia de cada caso.

La orden judicial que autorice la medida deberá fundamentar su necesidad, razonabilidad y proporcionalidad, justificando especialmente la ponderación de su utilidad con relación a la afectación de derechos fundamentales involucrados, la gravedad del hecho investigado y que no existen medios menos intrusivos de la intimidad del imputado y demás afectados que resulten útiles para alcanzar los mismos fines probatorios.

En ningún caso la actuación del agente encubierto digital podrá inducir, incitar o promover la comisión de un delito que no hubiera ocurrido sin su intervención. Toda actividad deberá desarrollarse con carácter reactivo, documentando exclusivamente conductas ya en ejecución o con indicios razonables de planificación previa.

Artículo 13. Vigilancia acústica. Podrá autorizarse la escucha y grabación en forma no ostensible, a través de medios técnicos, de las conversaciones privadas del imputado que tengan lugar fuera del domicilio de cualquiera de los interlocutores.

Artículo 14. Interceptación de las comunicaciones. Podrá autorizarse el acceso en forma no ostensible al contenido de las comunicaciones del imputado a través de la intervención de las terminales o de los medios de comunicación que utiliza habitual u ocasionalmente.

Las empresas que brinden el servicio de comunicación respectivo deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.

Artículo 15. Acceso remoto sobre equipos informáticos. Podrá autorizarse la utilización no ostensible de un software que permita o facilite el acceso remoto al contenido de ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos.

43

El Juez deberá exigir al Fiscal que precise los datos o archivos informáticos que se procura obtener con la medida y la forma en la que se procederá a su acceso y captación; la identificación del software

mediante el cual se ejecutará el control de la información, la individualización de los ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos que serán objeto de vigilancia; y la duración estimada de la medida.

El Fiscal deberá solicitar al Juez la ampliación de la medida de registro si advirtiera que los datos buscados están almacenados en otro dispositivo informático al que se tiene acceso desde el sistema originariamente autorizado.

Artículo 16. Utilización de dispositivos de captación de imágenes. El Juez podrá ordenar la obtención y grabación de imágenes del imputado en espacios públicos en forma no ostensible, por cualquier medio técnico.

Artículo 17. Vigilancia a través de dispositivos de seguimiento y de localización. Podrá el Juez, autorizar la utilización no ostensible, de dispositivos o medios técnicos de seguimiento y localización.

El Juez deberá exigir al representante del MPF que especifique el medio técnico que será utilizado.

Artículo 18. Prohibición respecto de terceros. Efectos inevitables. Las medidas de vigilancia no podrán ser autorizadas respecto de terceros ajenos a la investigación. Sin perjuicio de lo dispuesto en el primer párrafo, las medidas reguladas en este capítulo podrán llevarse a cabo aun cuando tuvieran efectos inevitables sobre terceros ajenos a la investigación.

Artículo 19. Registros y cadena de custodia. Las medidas del presente Capítulo serán registradas mediante cualquier medio técnico idóneo que asegure la valoración ulterior de la información obtenida. Los registros serán conservados por el representante del MPF, quien dispondrá las medidas

HONORABLE
LEGISLATURA
DE LA PROVINCIA
DEL CHUBUT

de seguridad correspondientes para asegurar su fidelidad, inalterabilidad y resguardar la cadena de custodia, de conformidad con el art. 178, 183 y concordantes del CPPCh.

El representante del MPF incorporará al legajo los registros referidos en el primer párrafo, siempre que tuvieran relación con el proceso, sea como prueba de cargo o de descargo.

Los registros que el representante del MPF considere que no son útiles para el proceso serán puestos a disposición de la defensa, con la debida preservación de la cadena de custodia. Si la defensa no tuviere interés en conservar tales registros, serán destruidos.

Todo aquel que tomare contacto con los elementos no incorporados al legajo deberá guardar secreto respecto de ellos.

Todo registro o copia debidamente protegida y autenticada que se realice deberá estar a disposición de las partes en todo momento para su control y contestación.

Artículo 20. La presente ley tiene carácter complementario del Código Procesal Penal de la Provincia del Chubut (Ley XVN°9 y modificatorias) y deberá interpretarse e integrarse armónicamente con sus disposiciones. En caso de silencio, insuficiencia o ausencia de regulación específica, resultarán de aplicación supletoria las previsiones de dicha ley, en cuanto sean compatibles con la naturaleza, objeto y principios de la presente ley.

43

Artículo 21. Ley General. Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DE LA HONORABLE LEGISLATURA DE LA PROVINCIA DEL CHUBUT, A LOS DOS DÍAS DEL MES DE MARZO DE DOS MIL VEINTISEIS.-

María Ligia MORELLI
Secretaria Legislativa
Honorable Legislatura del Chubut

Dr. Gustavo MENNA
Presidente
Honorable Legislatura del Chubut