MINISTERIO DE SEGURIDAD Y JUSTICIA
Ley Nº 9510

EL SENADO Y CÁMARA DE DIPUTADOS DE LA PROVINCIA DE MENDOZA,

SANCIONAN CON FUERZA DE

LEY:

Artículo 1°- Incorpóranse los artículos 29 bis, 224 bis, 224 ter y 228 bis, y modifícase el artículo 226 de la Ley 6730 –Código Procesal Penal - y sus modificatorias, los que quedarán redactados de la siguiente manera:

“Artículo 29 bis.- Agente encubierto digital. En los casos de investigación de delitos en que resulte necesaria la intervención del agente en entornos o plataformas digitales, el Fiscal podrá requerir fundadamente ante el Juez Penal Colegiado la actuación encubierta de un agente bajo las premisas anteriores y las condiciones aquí previstas. La autorización de este medio de investigación excepcional, se emitirá por decreto fundado, en el marco de la investigación de delitos previstos en los artículos 128, 131 del Código Penal, en delitos concretos de especial gravedad o de investigación compleja y siempre que existan motivos suficientes que acrediten:

a) Que el éxito de la investigación esté seriamente dificultado de no recurrirse a este medio,

b) Que se trata de delitos cometidos a través de medios informáticos que no permiten otra forma de investigación.

La actuación encubierta no podrá exceder de ciento ochenta (180) días a contar desde que la autorización otorgada por el Juez Penal sea notificada al Fiscal. Los perfiles o identidades digitales, en ningún caso podrán ser imágenes de personas reales, serán creados y administrados por personal técnico idóneo del Ministerio Público Fiscal, funcionarios o auxiliares de la fuerza de seguridad en función judicial con experiencia y desarrollo en la materia, y bajo el control directo del Fiscal a cargo de la investigación, quien hará constar las directivas, reservando en caja de seguridad: la denominación y características del perfil utilizado por el agente encubierto; plataformas digitales donde se actuará; claves de acceso validadas y actividad concreta a desarrollar por el agente. Una vez concluida la intervención del agente encubierto digital, el Fiscal dejará constancias de su existencia en el legajo/expediente.

El agente encubierto digital, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido. El agente encubierto digital estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de ésta y no constituyan una provocación al delito.

A los efectos del presente artículo se considera agente encubierto digital al funcionario de las fuerzas de seguridad o miembro del Ministerio Público Fiscal autorizado, que previo prestar su consentimiento, oculte o utilice un perfil digital encubierto, interactúe y se relacione digitalmente a través de tecnologías de la información y de la comunicación con el objeto de: identificar o detener a los autores, partícipes o encubridores de un delito; impedir la consumación de un delito; o para reunir información o elementos de prueba necesarios para la investigación.”

“Artículo 224 bis. - Orden de Presentación de Datos Informáticos. Siempre que se vincule con la investigación de un delito de su competencia, el Fiscal podrá ordenar por decreto fundado, a cualquier persona humana o jurídica en el territorio provincial, la presentación de datos informáticos, electrónicos o digitales o en un dispositivo de almacenamiento informático que obre en su poder o bajo su control, relativos a la identificación o localización u otra información asociada de un usuario y/o abonado, y que se pueda acceder al sistema legítimamente aunque no se encuentre dentro del territorio.

Asimismo, el Fiscal podrá ordenar a toda persona humana o jurídica que preste un servicio de comunicaciones o a los proveedores de Internet de cualquier clase en jurisdicción argentina, la entrega de datos personales o de identificación de los usuarios y/o abonados u otra información asociada, que tengan bajo su poder o a los que pueda acceder de manera legítima, aunque estén fuera de esa jurisdicción. La orden podrá contener la indicación de que la medida deberá mantenerse secreta bajo apercibimiento de sanción penal y con las limitaciones establecidas en el Art. 225 del C.P.P..

El destinatario quedará obligado a adoptar todas las medidas técnicas de seguridad necesarias, para mantener en secreto la medida ordenada por el Magistrado.”

“Artículo 224 ter. - Aseguramiento de Datos Informáticos almacenados. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro del territorio provincial pudieren ser alterados o suprimidos, el Fiscal podrá ordenar a cualquier persona humana o jurídica el aseguramiento de datos informáticos concretos y que estén a su disposición o para el que tiene legítimo acceso.

Dicho aseguramiento podrá consistir en la conservación rápida de datos informáticos almacenados y la conservación y revelación parcial rápida de datos relativos al tráfico.

La orden deberá especificar los datos concretos que se pretende conservar y la duración de la medida que no podrá exceder de noventa (90) días, prorrogables por igual periodo si se mantuvieren los motivos que fundamentaron la orden.

La persona requerida deberá mantener en secreto la medida bajo apercibimiento de sanción penal.”

“Artículo 228 bis. - Secuestro, Apertura y Análisis de Sistema Informático e Incautación de Datos. A pedido del Fiscal, el Juez Penal Colegiado podrá ordenar por decreto 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 secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las mismas condiciones establecidas en el Art. 216 del C.P.P. y con las limitaciones establecidas en el Art. 225 del C.P.P..

La ejecución de la actuación se hará bajo la responsabilidad del Fiscal que solicitó la medida.

El Fiscal deberá indicar al juez:

a) La individualización de los dispositivos o sistemas informáticos que serán objeto del registro,

b) Una descripción del objeto concreto de la medida,

c) La identificación de los mecanismos, metodología y herramientas mediante los cuales se almacenará la información obtenida que permitan asegurar la integridad de los datos y el resguardo de la cadena de custodia,

d) El funcionario y/o quien designe como encargada de la ejecución del registro, copia o incautación de datos.

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

En caso de que durante la ejecución de esta medida surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema conectado al inicial o estén disponibles para éste, dentro de la misma jurisdicción, quienes lleven adelante la medida podrán extenderla o ampliar el registro al otro sistema, previa comunicación con el agente Fiscal, quien deberá solicitar autorización telefónica del Juez Penal Colegiado competente. La mencionada comunicación no podrá ser delegada por el Fiscal de Instrucción a ningún funcionario judicial. El Juez, por decreto fundado deberá disponer la autorización o rechazo de la medida, notificándola por correo electrónico y/o en forma telefónica. En caso que la medida sea autorizada, el agente Fiscal deberá acompañar por escrito la solicitud fundada dentro de las 48 horas de realizada la medida. En caso de ser necesario, por la complejidad del asunto el Juez podrá librar la orden, consignando únicamente su parte dispositiva, difiriéndose los fundamentos de las mismas. Ésta se efectuará, bajo pena de nulidad, en el plazo máximo de 24 horas a contar del momento de autorización de la orden.

En los supuestos en que los datos se encuentren almacenados en otra jurisdicción, la medida de registro de datos podrá ampliarse a dispositivos o sistemas informáticos, sólo en los siguientes supuestos:

a) Cuando se obtenga el consentimiento voluntario y lícito de la persona con facultades para disponer de la revelación de los datos desde el dispositivo o sistema informático inicial al que se accedió legalmente.

b) Cuando resulte posible recibir o acceder a los datos buscados desde el sistema original sin necesidad de realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en otro Estado.

c) Cuando por la estructura del sistema informático no resulte posible determinar en forma certera al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados físicamente y no resulte necesario para acceder a ellos de la realización de maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en otro Estado.

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

Una vez concluido el Proceso Penal, por sentencia firme, se dispondrá la devolución de los dispositivos electrónicos secuestrados, que no fueren objeto de decomiso previa eliminación del material ilícito.

Si en estricto cumplimiento de la ejecución de las medidas se encontraren de modo casual datos o archivos informáticos que evidencien la comisión de un delito distinto al que motivó la medida, se procederá a su secuestro y se comunicará al Fiscal interviniente."

"Artículo 226.- Custodia o Depósito. Los efectos secuestrados serán inventariados y puestos bajo segura custodia a disposición del magistrado interviniente, o se ordenará su depósito.

Cuando se tratare de automotores u otros bienes de significativo valor, no se entregarán en depósito sino a sus propietarios, salvo que desde su secuestro hayan transcurrido seis (6) meses sin que hubiere mediado reclamo por parte de aquellos.

Los automotores podrán ser solicitados en depósito al órgano judicial interviniente, por el Poder Ejecutivo - a través de funcionario que éste designe- para ser afectados exclusivamente al cumplimiento de la función de seguridad que compete a la Policía de la Provincia o por el Procurador General para ser destinados a la tarea de la Policía en función Judicial.

Los dispositivos electrónicos podrán ser solicitados en depósito al magistrado interviniente, por el Poder Ejecutivo, a través de funcionario que éste designe, para ser afectados exclusivamente al cumplimiento de la función de seguridad que compete a la Policía de la Provincia a través de la División Investigaciones o la que en su futuro la reemplace o por el Procurador General para ser destinados a la tarea del Ministerio Público Fiscal o a los Laboratorios Forenses.

Se podrá disponer la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la investigación penal preparatoria.

Las cosas secuestradas serán aseguradas con faja de seguridad o mediante sistema de protección adecuado y sello del Tribunal o Fiscalía que intervenga, con la firma del Juez o Fiscal según corresponda y la firma del Secretario, debiéndose firmar los documentos en cada una de sus hojas. Durante todo el procedimiento se deberán tomar las medidas necesarias y conducentes a fin de asegurar la cadena de custodia e integridad de las evidencias colectadas, dejando debido registro de todas las intervenciones realizadas sobre el material secuestrado."

Art 2º- Comuníquese al Poder Ejecutivo.

DADA EN EL RECINTO DE SESIONES DE LA HONORABLE LEGISLATURA, en Mendoza, a los treinta días del mes de enero del año dos mil veinticuatro.

DRA. HEBE CASADO

LIC. ANDRÉS LOMBARDI

LIC. LUCAS ADRIÁN FAURE

DRA. MARÍA CAROLINA LETTRY

Publicaciones: 1

Fecha de Publicación	Nro Boletín
04/03/2024	32061