Expte Nro.: 0000072000

FUNDAMENTOS

HONORABLE CAMARA:

El presente proyecto de Ley tiene por objeto modificar el Código Procesal Penal de la Provincia de Mendoza, la presente propuesta de reforma está enmarcada dentro de una serie de iniciativas afrontadas a nivel nacional en materia de cibercriminalidad y obtención de evidencia digital.

El 15 de diciembre de 2017, nuestro país aprobó por ley la Convención de Budapest sobre Ciberdelito adoptada en la Ciudad de Budapest, Hungría, el 23 de noviembre de 2001, ante la necesidad de aplicar una política penal común a nivel internacional, con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación penal sustantiva y procesal adecuadas, y la mejora de la cooperación internacional en la lucha contra el cibercrimen.

Previo a la aprobación de la Convención, nuestro país fue adecuando la ley penal sustantiva, incorporando delitos vinculados a la cibercriminalidad informática. Fue así que el 4 de junio de 2008 se sanciona la Ley Nº 26.388, denominada “Ley de Delitos Informáticos”, modificatoria del Código Penal argentino, mediante la cual se tipifican los llamados ciberdelitos, tales como la ciberpornografía infantil, la violación, apoderamiento y desvío de comunicaciones electrónicas, la interceptación o captación de las mismas, el acceso indebido a un sistema o dato informático, la publicación indebida de una comunicación electrónica, la revelación de datos que por ley deben ser secretos, el acceso indebido a un banco de datos personales, la inserción de datos falsos en un archivo de datos personales, las defraudaciones por el uso ilícito de tarjeta de crédito o débito, la defraudación informática, el daño informático.

Posteriormente, en el año 2013, se sanciona la Ley de Grooming, bajo el Nº 26904, que viene a tipificar el delito de abuso sexual digital perpetrado contra personas menores de edad por medio de comunicaciones electrónicas

Finalmente, en marzo de 2018, el Congreso aprobó la ley Nº 27.436, que penaliza la tenencia de pornografía infantil.

Sin embargo, más allá de la incorporación al Código Penal argentino de estos ciberdelitos, la tecnología y la digitalización, sumadas a la convergencia y la globalización continuas de las redes sociales, han complejizado también la comisión y

prueba de los que podrían llamarse delitos “tradicionales” tales como las calumnias e injurias, las amenazas, la extorsión, la intimidación pública, la instigación al suicidio, sólo por mencionar algunos. Ocurre que la tecnología ha atravesado nuestras vidas, se ha hecho parte de nuestra cotidianeidad, y hoy el componente informático está presente en la comisión de todos los tipos delictivos, desafiando a quienes deben procurar la investigación y persecución de los mismos, a recabar y analizar evidencia digital.

Por ello, si bien en materia de derecho penal sustancial, Argentina ha ido dando cumplimiento a las exigencias de la Convención de Budapest, es en la exigencias a nivel de derecho procesal penal que nos hemos ido quedando atrasados respecto a la evolución tecnológica.

Atento que el dictado de los códigos de forma es materia no delegada en la Nación, es competencia legislativa de cada provincia llevar a cabo la tarea de aggiornar los Códigos Procesales en materia penal, dando cumplimiento a las exigencias de la Convención de Budapest, para poder investigar y perseguir los delitos informáticos y aquellos que sin serlo, tienen el componente informático en su comisión.

Nuestro Código Procesal Penal si bien tiene reglas relativas a medidas de prueba tales como el registro, el allanamiento, el secuestro, la requisa personal y la interceptación de comunicaciones; la aplicación de las mismas a la evidencia digital no es posible, pues el desafío que plantea el tratamiento de la misma requiere de medidas de prueba específicas, o la adaptación legal de las ya existentes.

Si bien el Código Procesal Penal establece en su artículo 205 el principio de libertad probatoria, este debe ser interpretado a la luz de la máxima *nulla coactio sine lege*, que tiene recepción en nuestro ordenamiento procesal en el artículo 2, que exige interpretar restrictivamente las disposiciones legales que coarten la libertad personal o limiten el ejercicio de un poder o derecho conferido a los sujetos del proceso, y prohíbe la interpretación extensiva y la analogía mientras no favorezcan la libertad del imputado ni el ejercicio de una facultad conferida a quienes intervienen en el procedimiento.

Es que la aplicación analógica deja sujeta a la interpretación de los operadores de justicia la aplicación de medidas de prueba, impidiendo la existencia de estándares generalizados de judicialidad, motivación, proporcionalidad y legalidad al momento de recabar, tratar y valorar la prueba digital.

Dicho esto, y de acuerdo a lo expresado por la Comisión Interamericana de Derechos Humanos en el Informe 38/96, párrafo 60, si una medida afecta derechos protegidos por

la Convención Interamericana de Derechos Humanos, esta debe estar necesariamente prescrita por ley. Esa es la concreción de la máxima *nulla coactio sine lege.*

Hoy en día acceder a un dispositivo tecnológico es mucho más invasivo que allanar un domicilio, los derechos de intimidad y privacidad pueden ser absolutamente vulnerados al acceder por ejemplo, a un *smartphone* secuestrado, pues las personas allí almacenan datos e información absolutamente privados y sensibles. Es por ello que para ordenar el acceso a un dispositivo tecnológico que permita almacenar datos informáticos, se hace indispensable que la ley expresamente prevea una medida para hacerlo, pues implica una injerencia a la vida privada de las personas, y si no está legalmente establecida, la misma resultaría arbitraria.

Es por ello que el presente proyecto persigue actualizar nuestro Código Procesal Penal a los tiempos que corren, para enfrentar los desafíos que la tecnología plantea a la hora de perseguir e investigar delitos, sean estos ciberdelitos o delitos tradicionales cuyo rastro es digital.

También fundamenta la reforma que se propone mediante el presente, la importancia de que la incorporación al procedimiento de la prueba sea legal, pues si la prueba que se agrega al proceso ha sido recabada en detrimento de garantías y derechos constitucionales, dicha prueba estaría viciada. De manera que, procurando amparar derechos y garantías de las personas ante el poder coercitivo del Estado, también se asegura un procedimiento transparente y válido.

Es por ello que se propone reformar aquellos artículos que consagran medidas probatorias que suponen una injerencia en la vida privada de las personas, así como también se propone añadir nuevas medidas de prueba y conservación exclusivas para el caso de tener que recabar y analizar evidencia contenida en dispositivos tecnológicos o en sistemas informáticos.

Se propone reformar el artículo 216, en cuanto la medida de registro de un lugar o espacio físico, no legitima en sí misma al registro de dispositivos informáticos hallados en el lugar; para acceder a los mismos y registrarlos o hacer sobre ellos una pericia informática, se requiere una autorización expresa del juez competente. Ello resguarda la intimidad del titular o usuario del dispositivo electrónico o sistema informático y, a su vez se evitan accesos espontáneos a los sistemas informáticos en el momento del registro, que pueden alterar la evidencia digital y viciarla. Ello se refuerza con la reforma propuesta al artículo 337 del Código.

Por ello es que se propone incorporar dos artículos, el 216 bis y el 216 ter, los cuales se refieren específicamente al registro de dispositivos tecnológicos que contienen evidencia digital. El primero de los artículos refiere al registro físico, el segundo al registro remoto o registro digital.

En el caso del registro físico, se requiere una autorización expresa del juez para poder acceder y realizar una copia forense del dispositivo, sobre la cual posteriormente podrán registrarse los datos informáticos allí contenidos en busca de los que sean pertinentes a la investigación.

El registro remoto es una medida de mayor injerencia en la privacidad de quien la soporta, por ello su solicitud deberá ser autorizada sólo en casos urgentes, cuando se trate de delitos graves, en los que la vida o integridad física o sexual de una persona estén seriamente comprometidos. Asimismo, la medida debe estar debidamente fundada, debe ser necesaria y proporcional.

También se propone modificar el artículo 223, para dejar expresamente establecida la posibilidad de confiscar datos informáticos almacenados, tal como exige el artículo 19 de la Convención de Budapest. Para ello el tribunal puede disponer su secuestro, lo que implica la copia de los datos informáticos almacenados y la posibilidad de hacerlos inaccesibles del sistema informático o el dispositivo tecnológico. Lo que no se ha admitido en la propuesta de reforma es la posibilidad de suprimir los datos, ello atento lo establecido por el artículo 230 del Código de rito, cuya reforma también se propone.

En el artículo 224 se propone incorporar la posibilidad de que los datos informáticos, los nombres de usuario y contraseñas necesarios para entrar a un sistema informático o los dispositivos de almacenamientos informático sean entregados o facilitados voluntariamente por quien los conozca o tenga bajo su poder, para evitar hacerlo coercitivamente.

En los artículos 224 bis, ter y quater se propone incorporar medidas exclusivamente aplicables al tratamiento de la evidencia digital. En el artículo 224 bis se admite expresamente la posibilidad de solicitar la conservación rápida de datos informáticos a proveedores de servicio, para que estos no sean alterados en el transcurso de la investigación. Cabe aclarar que la mera conservación no implica el acceso a esos datos, por ello no se diferencia respecto a la calidad de los datos, pueden ser datos básicos, datos de tráfico o de contenido.

Tal como lo establece la Convención de Budapest, se autoriza a obligar a quien debe

efectuar la conservación a mantener en secreto la misma, de manera que el usuario o abonado no advierta la medida.

Luego se avanza en los artículos siguientes y se propone la posibilidad de solicitar y acceder a esos datos cuya conservación se ha solicitado y que obran en poder de un proveedor de servicios. Para ello se distinguen los datos según su naturaleza, pues dependiendo de la misma es el estándar de convicción requerido, ya que el acceso a determinados datos supone una injerencia menor en la privacidad y en el caso de otros la injerencia es absoluta.

Cabe aclarar que los datos informáticos de usuarios y/o abonados en poder de un proveedor de servicios pueden ser de tres tipos: Básicos, de Tráfico, de Contenido.

Según la Convención de Budapest (artículo 18), los *"datos básicos"* son los que permiten determinar:

1. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;
2. 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;
3. 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.

Según la Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero, confeccionada por la Unidad Fiscal Especializada en Ciberdelincuencia, perteneciente al Ministerio Público Fiscal de la Nación y la Dirección General de Cooperación Regional e Internacional, la *"información básica del suscriptor"* incluye:

1. Datos del titular de la cuenta (nombre, país, dirección, teléfonos, edad, género)
2. Dirección de correo electrónico asociada
3. Número de teléfono celular asociado
4. Número de tarjeta de crédito asociada
5. Dirección IP desde la que se creó la cuenta
6. Detalle de los últimos accesos a la cuenta (fecha, hora, zona horaria y dirección IP)
7. Información sobre servicios a los que se ha suscripto el titular de la cuenta

Por su parte, los *"datos de tráfico"* del destinatario incluyen:

1. Datos de remitente y receptor de correos electrónicos y sus direcciones IP de conexión
2. Día y hora de las comunicaciones que se efectuaron
3. Cantidad de datos que insumió la comunicación
4. Sitios web visitados por los usuarios

Finalmente, la *"información de contenido"* incluye:

1. Contenido (textos y adjuntos) de los correos electrónicos que permanezcan en las carpetas de la cuenta (enviados, recibidos, borrador, papelera)
2. Contenido (texto y adjuntos) de los mensajes intercambiados en plataformas de redes sociales
3. Contenido de publicaciones realizadas en redes sociales cuyo acceso fue restringido al público en general
4. Historial de localización asociado a la cuenta
5. Fotos y otros documentos almacenados por el usuario en espacios de alojamiento en la nube asociados a una cuenta.

Dado que en el caso de estos dos últimos tipos de datos la injerencia en la vida privada y el acceso a información íntima y sensible es absoluto, el estándar de convicción debe ser el más alto, al igual que la medida coercitiva de allanamiento de morada y debe basarse en una causa probable actual.

Se introduce también una pequeña modificación en el artículo 226, previendo expresamente la posibilidad de realizar copias forenses o "copia bit a bit" de los dispositivos tecnológicos que contienen evidencia digital.

Por otra parte, se propone reformar el artículo 229, adaptándolo a las exigencias de la Convención de Budapest respecto a la obtención en tiempo real de datos relativos al tráfico y a la interceptación de datos relativos al contenido. La propuesta de reforma tiene como fin dejar expresamente establecida en la ley la posibilidad de tomar estas medidas, puesto que como se encuentra actualmente redactado el artículo, podría inferirse que estas medidas pueden ser adoptadas, al permitir la intervención de comunicaciones, cualquiera sea el medio técnico utilizado, sin embargo, como ya se expresó al principio de estos fundamentos, una medida coercitiva de esta naturaleza, debe preverse expresamente en la ley, en función de la máxima *nulla coactio sine lege.*

Finalmente, se propone la introducción, en el artículo 29, de la figura del agente encubierto informático, figura a la que sólo se podrá recurrir en determinados delitos y

que puede ser muy útil en la lucha contra la pornografía infantil y el delito de grooming.

Teniendo en Cuenta que los Objetivos del Desarrollo Sostenible han propuesto un marco de acción convalidado por 193 países, de los 17 objetivos establecidos, este proyecto se enmarca en el Objetivo 16 Paz, Justicia e Instituciones Sólidas, en sus metas:

16.2 Poner fin al maltrato, la explotación, la trata y todas las formas de violencia y tortura contra los niños

16.3 Promover el estado de derecho en los planos nacional e internacional y garantizar la igualdad de acceso a la Justicia para todos .

En Mendoza, desde distintas organizaciones de la Sociedad Civil se está trabajando la temática de prevención de grooming, pero aún falta que el Estado tenga estas herramientas necesarias en la Justicia para dar respuesta eficiente y eficaz ante cada denuncia y dar con los responsables de la realización de estos delitos.

Para el desarrollo de la presente propuesta se ha contado con el asesoramiento profesional de la Dra. Bárbara Virginia Peñaloza, abogada, Matrícula, 7382 especialista en derecho informático y del Fiscal de Delitos Económicos, Dr. Santiago Garay.

Por lo anteriormente expuesto es que solicito a las señoras senadoras y a los señores senadores la aprobación del presente proyecto de Ley.

Mendoza 30 de Octubre 2018

PROYECTO DE LEY
EL SENADO Y CAMARA DE DIPUTADOS DE LA PROVINCIA DE MENDOZA SANCIONAN CON FUERZA DE
L E Y:

Artículo 1º: Modifícase el artículo 216 del Código Procesal Penal de la Provincia de Mendoza, que quedará redactado de la siguiente manera:

Artículo 216. Registro.

Si hubiere motivos suficientes para presumir que en determinado lugar existen cosas pertinentes al delito, o que allí puede efectuarse la detención del imputado o de alguna persona evadida o sospechada de criminalidad, el tribunal o fiscal de instrucción si no fuere necesario allanar el domicilio, ordenarán por decreto fundado, bajo pena de nulidad, el registro de ese lugar. Podrán también disponer de la fuerza pública y proceder

personalmente o delegar la diligencia en funcionarios de la policía judicial. En este caso, la orden, bajo pena de nulidad, será escrita, expresando el lugar, día y hora en que la medida deberá efectuarse y el nombre del comisionado, quien actuará conforme al capítulo 2 del presente título. Excepcionalmente, y siempre que hubiera motivos suficientes y razonablemente fundados para presumir el ocultamiento de armas, municiones, explosivos o cosas presuntamente relacionadas con la comisión del delito en un determinado lugar, complejo residencial o habitacional, barrio o zona determinada, el magistrado competente podrá disponer de la fuerza pública para proceder al registro, debiendo ordenar in situ, si correspondiere, el allanamiento de lugares determinados mediante decreto firmado. La diligencia deberá contar, bajo pena de nulidad, con la presencia del funcionario del ministerio público competente.

Cuando en ocasión de la realización de un registro sean hallados dispositivos tecnológicos que pudieran contener evidencia digital, el secuestro de los mismos no autoriza, en ningún caso, el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el Juez de Garantías interviniente.

Art. 2º: Incorpórese el art. 216 bis: “Registro de dispositivos tecnológicos que contengan evidencia digital”.

Si hubiere motivos suficientes para presumir que en los dispositivos tecnológicos o en los sistemas informáticos a registrar, existe evidencia digital pertinente a la investigación delito, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, ordenará por decreto fundado, bajo pena de nulidad, el acceso a ese dispositivo o sistema para ser registrados los datos informáticos allí contenidos, y, de ser posible, la realización previamente de una copia forense del mismo. La orden deberá fijar los términos y el alcance de la misma.

Cuando quienes lleven a cabo el registro o tengan acceso al dispositivo o sistema de información o a una parte del mismo, tengan motivos suficientes para considerar que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, situado en territorio nacional, podrán ampliar el registro, siempre que los datos sean legítimamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el tribunal, salvo que ya lo hubiera sido en la autorización inicial.

Art. 3º: Incorpórese el artículo 216 ter: “Registro remoto de dispositivos tecnológicos que contengan evidencia digital”.

En supuestos urgentes, tratándose de delitos graves, previstos en los artículos 83, 140, 141, 142, 142 bis, 145, 145 bis, 145 ter, 146, 147 y 170 en el Título III del Código Penal

de la Nación, cuando esté en riesgo la vida, la libertad o la integridad sexual de las personas, si hubiere motivos suficientes para presumir que en determinado dispositivo tecnológico o en un sistema informático, existe evidencia digital pertinente a la investigación delito, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción**,** ordenará por decreto fundado, bajo pena de nulidad, el registro remoto de ese dispositivo mediante la instalación de un software que permita el examen a distancia de datos informáticos de existencia previa al registro, contenida en el dispositivo tecnológico.

La orden debe ser escrita y fundada y deberá especificar: a) Los dispositivos tecnológicos objeto de la medida. b) El alcance de la misma y el software mediante el que se ejecutará el control de la información. c) Los agentes autorizados para la ejecución de la medida. d) Dia y hora en que se realizará la medida e) Duración de la medida, que no podrá exceder de un plazo de 48 hs.

Cuando quienes lleven a cabo el registro remoto, tengan motivos suficientes para considerar que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, situado su territorio nacional, podrán ampliar el registro, siempre que los datos sean legítimamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el tribunal, salvo que ya lo hubiera sido en la autorización inicial.

Art. 4º: Modifícase el artículo 223 que quedará redactado de la siguiente manera:

Artículo 223. Orden de secuestro

El tribunal o el fiscal de instrucción, si no fuere necesario allanar domicilio, podrán disponer que sean conservadas o recogidas las cosas relacionadas con el delito, las sujetas a confiscación, aquéllas que puedan servir como prueba; también podrá disponer la realización y conservación de copias de datos informáticos almacenados en dispositivos o sistemas informáticos y determinar la inaccesibilidad a los mismos; para ello, cuando fuere necesario, se ordenará su secuestro. En casos urgentes, esta medida podrá ser delegada en un funcionario de la policía judicial en la forma prescrita para los registros.

Art. 5º: Modifícase el artículo 224, que quedará redactado de la siguiente manera:

Artículo 224. Orden de presentación. Limitaciones

En vez de disponer el secuestro se podrá ordenar, cuando fuere oportuno, la presentación o facilitación de los objetos, documentos o datos informáticos a que se refiere el artículo anterior. Asimismo, se podrá ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria para poder acceder a los mismos.

Esta orden no podrá dirigirse a las personas que deban abstenerse de declarar como testigos, por razón de parentesco, secreto profesional o de estado.

Art. 6º: Incorpórese el artículo 224 bis: “Orden de conservación rápida de datos informáticos almacenados”

Cuando existan motivos suficientes para creer que ciertos datos informáticos serán susceptibles de pérdida o de modificación, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, podrá ordenar, por decreto fundado, a cualquier persona física o jurídica la conservación rápida y protección de la integridad de datos informáticos específicos de usuarios y/o abonados, ya sea que estos constituyan información básica, de tráfico o de contenido, almacenados por medio de un sistema informático.

El tiempo durante el cual se deben conservar los datos no podrá exceder los noventa días, prorrogables por única vez por igual término.

El destinatario de la orden quedará obligado a adoptar todas las medidas técnicas de seguridad necesarias para mantener en secreto la ejecución de la conservación.

Art. 7º: Incorpórese el artículo 224 ter: “Orden de presentación de datos informáticos básicos de usuarios y/o abonados”.

El el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, podrá ordenar, por decreto fundado, a cualquier persona física o jurídica que presente datos informáticos almacenados en un sistema informático o en un dispositivo de almacenamiento informático, que obren en su poder o bajo su control, relativos a la identificación y localización de un usuario o abonado.

El destinatario quedará obligado a adoptar todas las medidas técnicas de seguridad necesarias para mantener en secreto la ejecución de la conservación.

Art. 8º: Incorpórese el artículo 224 quater: “Orden de presentación de datos informáticos de tráfico y de contenido de comunicaciones específicas de usuarios y/o abonados conservados por prestadores de servicios”

Cuando hubiere motivos suficientes para presumir que ciertos datos informáticos de tráfico y/o de contenido de comunicaciones específicas y de existencia previa a la orden, conservados por prestadores de servicios en archivos automatizados, son indispensables para la investigación de un delito, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, podrá ordenar, por decreto fundado, bajo pena de nulidad, a cualquier persona física o jurídica a que presente dichos datos.

El destinatario quedará obligado a adoptar todas las medidas técnicas de seguridad necesarias para mantener en secreto la ejecución de la conservación.

Art.9º: Modifícase el artículo 226, que quedará redactado de la siguiente manera:

Artículo 226. Custodia o depósito

Los efectos secuestrados serán inventariados y puestos bajo segura custodia, la disposición del órgano judicial 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 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 del funcionario que 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 judicial.

Se podrá disponer la obtención de copias o reproducciones de las cosas secuestradas, y copias forenses de los dispositivos tecnológicos secuestrados, cuando puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la investigación penal preparatoria.

Las cosas secuestradas serán aseguradas con el sello del tribunal o fiscalía de instrucción que intervenga y con la firma del juez o del fiscal, según corresponda, y 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.

Si fuera necesario remover los sellos, se verificará previamente su identidad e integridad. Concluido el acto, aquéllos serán repuestos, y todo se hará constar.

Art. 10º: Modifícase el artículo 229 que quedará redactado de la siguiente manera:

Artículo 229. Intervención de comunicaciones

El tribunal podrá ordenar por decreto fundado, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado, para impedirlas o conocerlas.

En supuestos urgentes, tratándose de delitos graves, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, podrá autorizar la obtención en tiempo real de datos relativos al tráfico de comunicaciones electrónicas específicas y el acceso en tiempo real al contenido de comunicaciones electrónicas específicas en las que participe el imputado, ya sea como emisor o como receptor, cualquiera sea el medio técnico utilizado.

Art. 11º: Modifícase el artículo 230 que quedará redactado de la siguiente manera:

Artículo 230. Devolución

Los objetos secuestrados que no estén sometidos a confiscación, restitución o embargo, serán devueltos, tan pronto como no sean necesarios, a la persona de cuyo poder se sacaron. Asimismo, respecto a datos o sistemas informáticos secuestrados, se habilitará la accesibilidad a los mismos, cuando se hubiera decretado su inaccesibilidad.

Esta devolución podrá ordenarse provisionalmente, en calidad de depósito, e imponerse al poseedor la obligación de exhibirlos. Los efectos sustraídos serán devueltos, en las mismas condiciones y según corresponda, al damnificado o al poseedor de buena fe de cuyo poder hubieran sido secuestrados.

Art. 12º: Modifícase el artículo 29 agregando la figura del Agente Encubierto Informático, quedará redactado de la siguiente manera:

Artículo 29: Actuación encubierta.

El fiscal de instrucción o el Juez de Garantías en su caso, podrá, por resolución fundada, de manera permanente o durante una investigación, por un delito con pena mayor de tres años, autorizar que una persona, o agente de policía, actuando de manera encubierta a los efectos de comprobar la comisión de algún delito o impedir su consumación, o lograr la individualización o detención de los autores, cómplices o encubridores, o para obtener o asegurar los medios de prueba necesarios, se introduzca como integrante de alguna organización delictiva, o actúe con personas que tengan entre sus fines la comisión de delitos y participe de la realización de algunos de los hechos previstos en el Código Penal y Leyes especiales de este carácter.

La designación deberá consignar el nombre verdadero del agente y la falsa identidad con la que actuará en el caso, y será reservada fuera de las actuaciones y con la debida seguridad.

La información que el agente encubierto vaya logrando será puesta de inmediato en conocimiento del juez.

La designación de un agente encubierto deberá mantenerse en estricto secreto. cuando fuere absolutamente imprescindible aportar como prueba la información personal del agente encubierto, éste declarará como testigo, sin perjuicio de adoptarse, en su caso, las medidas de protección necesarias.

El agente encubierto que como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que éste no implique poner en peligro cierto la vida o la integridad física de una persona o la imposición de un grave sufrimiento físico o moral a otro; al momento de resolver sobre su situación procesal, el magistrado interviniente deberá analizar si el agente encubierto ha actuado o no, conforme al Artículo 34 inc. 4) del Código Penal argentino, en virtud de las instrucciónes recibidas al momento de su designación; y decidirá en consecuencia.

Cuando el agente encubierto hubiese resultado imputado en un proceso, hará saber confidencialmente su carácter al magistrado interviniente, quien en forma reservada recabará la pertinente información a la autoridad que corresponda.

Si el caso correspondiere a previsiones del primer párrafo de este Artículo, el juez resolverá sin develar la verdadera identidad del imputado.

Ningún agente de las fuerzas de seguridad podrá ser obligado a actuar como agente encubierto. la negativa a hacerlo no será tenida como antecedente desfavorable para ningún efecto.

Cuando peligre la seguridad de la persona que haya actuado como agente encubierto por haberse develado su verdadera identidad, sin perjuicio de las medidas protectivas que para el mismo, y/o su familia, y/o bienes deberán disponerse, tendrá derecho a seguir percibiendo su remuneración bajos las formas que el magistrado interviniente seale tendientes a la protección de la gente. si se tratare de un particular, percibirá una retribución similar a la de un agente público, conforme al criterio anteriormente expuesto.

Agente encubierto informático

El Juez de Garantías, a pedido del Fiscal de Instrucción podrá autorizar la actuación del agente encubierto informático, siempre que persiga la investigación de delitos cometidos a través de medios informáticos o de cualquier otra tecnología de la información o la comunicación.

Será considerado agente encubierto informático el funcionario de las fuerzas de seguridad autorizado judicialmente, que prestando su consentimiento y ocultando su identidad o utilizando una supuesta o falsa, interactúe y se relacione digitalmente, a través tecnologías de la información y comunicación, con el fin de identificar o detener a los autores, partícipes o encubridores de un delito, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación.

Los perfiles que utilice el agente en la medida serán regulados y administrados por el Ministerio Público Fiscal, debiendo dejar constancia de toda la información necesaria para poder acceder a los mismos.

Art. 13º: Modifícase el artículo 337, que quedará redactado de la siguiente manera:

Artículo 337. Prohibiciones
Los oficiales y auxiliares de la policía judicial no podrán abrir la correspondencia, ni podrán acceder a los dispositivos tecnológicos que resguarden o hubieran secuestrado por orden de autoridad judicial competente, sino que los remitirán intactos a ésta. Sin embargo, en los casos urgentes podrán ocurrir a la más inmediata, la que autorizará la apertura o acceso si lo creyere oportuno. Tampoco podrán difundir en los medios de comunicación los nombres y fotografías de las personas investigadas como participantes de un hecho, salvo que mediare expresa autorización del órgano judicial competente.

Art. 14º: De forma.