CÁMARA DE DIPUTADOS
MESA DE MOVIMIENTO
21 MAY 2024
Recibido 11:15 Hs.
Exp. Nº 53880 C.D.

LA LEGISLATURA DE LA PROVINCIA DE SANTA FE SANCIONA CON FUERZA DE LEY:

INCORPORACIONES EN MATERIA DE CIBER CRIMINALIDAD Y OBTENCIÓN DE EVIDENCIA DIGITAL.

Artículo 1°: Modifíquese el Artículo 169 del Código Procesal Penal de la Provincia de Santa Fe, el que quedará redactado de la siguiente manera:

"Artículo 169.- Allanamiento. Cuando el registro deba efectuarse en lugar habitado, casa de negocio o en sus dependencias y siempre que no se contara con la autorización libre y previamente expresada por quien tenga derecho a oponerse, el Tribunal, a solicitud fundada, autorizará el allanamiento con la mayor celeridad posible.

La medida podrá ser cumplida personalmente por el Juez, o en su defecto éste expedirá autorización escrita en favor del Fiscal, o del funcionario judicial o policial a quien se delegue su cumplimiento, y comunicada por cualquier medio, incluso electrónico o informático. Si la diligencia fuera practicada por la Policía será aplicable en lo pertinente el artículo 268 inciso 6) y la diligencia deberá ser filmada desde el inicio del procedimiento. El Juez podrá, de manera fundada, eximir el cumplimiento del recaudo de filmación. La diligencia deberá autorizarse individualizando los objetos a secuestrar o las personas a detener. En cuanto a los objetos, podrá prescindirse de dicha individualización, dando suficientes razones de tal imposibilidad, brindando todos los detalles conducentes a la misma.

La diligencia sólo podrá comenzar entre las siete (7) y las veintiún (21) horas Sin embargo, se podrá autorizar a proceder en cualquier

hora cuando el interesado o su representante lo consientan, o en los casos graves y que no admitan demora por el riesgo de frustrarse la investigación, o cuando peligre el orden público. La autorización del allanamiento será exhibida al que habita u ocupa el lugar donde deba efectuarse, o cuando estuviere ausente, a su encargado a falta de éste, a cualquier persona mayor de edad que se hallare en el lugar, prefiriendo a los familiares del primero. A la persona se le invitará a presenciar el registro. Cuando no se encontrare a nadie, ello se hará constar en el acta. Si en el acto se hallaren objetos que presumiblemente estuvieran relacionados a otros hechos delictivos o armas de fuego cuya tenencia no estuviera legalmente justificada, deberán ser secuestrados informando al Juez.

El secuestro de dispositivos tecnológicos en el marco de un allanamiento no autoriza, en principio, al acceso a su contenido, sin perjuicio de que éste pueda ser autorizado por el Juez, conforme las disposiciones de este Código.

Practicado el registro, se consignará en el acta su resultado, con expresión de todas las circunstancias útiles para la investigación. El acta será firmada por los concurrentes. Si alguien no lo hiciere se expondrá la razón.

La autorización no será necesaria para el registro de los edificios públicos y oficinas administrativas, los establecimientos de reunión o de recreo, el local de las asociaciones, cualquier otro lugar cerrado que no esté destinado a habitación o residencia particular. En estos casos deberá darse aviso a las personas a cuyo cargo estuvieren los locales, salvo que ello fuere perjudicial a la investigación.

Cuando para el cumplimiento de sus funciones o por razones de

higiene, para prevenir daños ambientales o inundaciones, moralidad u orden público, alguna autoridad nacional, provincial, municipal o comuna competente necesite practicar registros domiciliarios, solicitará directamente al Juez autorización de allanamiento, expresando los fundamentos del pedido. El Juez resolverá la solicitud pudiendo requerir que se amplíe la información que se estime pertinente y ordenará los recaudos para su cumplimiento.-"

Artículo 2°: Modifíquese el Artículo 171 del Código Procesal Penal de Santa Fe, el que quedará redactado de la siguiente manera:
"Artículo 171.- Interceptación de correspondencia e intervención de comunicaciones. El Tribunal, a pedido de partes, podrá autorizar por decreto fundado, la interceptación o el secuestro de la correspondencia postal, telegráfica o electrónica, o de todo otro efecto remitido o destinado al imputado o a terceros, aunque sean bajo nombres supuestos.
Del mismo modo, se podrá autorizar la intervención de las comunicaciones del imputado o de terceros, cualquiera sea el medio técnico utilizado, para impedirlas o conocerlas.
La intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo máximo de treinta (30) días, pudiendo ser renovada, expresando los motivos que justifican la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado. La solicitud deberá indicar el plazo de duración que estime necesario según las circunstancias del caso. El juez controlará la legalidad y razonabilidad del requerimiento y resolverá fundadamente.

Rige para los magistrados, funcionarios, agentes y empleados que tengan participación activa en la intervención o responsabilidad sobre los elementos probatorios, el deber de confidencialidad y secreto respecto de la información obtenida por estos medios. Quienes incumplan este deber incurrirán en responsabilidad penal. Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.

Si desaparecieren las circunstancias tenidas en cuenta para justificar la intervención de las comunicaciones, se hubiera agotado el plazo de duración, se hubiere cumplido el objetivo o resultare evidente que el objetivo pretendido no puede alcanzarse, la medida deberá ser interrumpida inmediatamente."

Artículo 3°: Incorpórese el Artículo 204 Octies "Agente encubierto informático", con la siguiente redacción:

"Art. 204 Octies – Agente encubierto informático. En los casos de investigación de hechos presuntamente delictivos en que resultare necesaria la intervención del agente en entornos o plataformas digitales, el Fiscal podrá requerir ante el Juez la actuación de un agente encubierto informático para que, ocultando su identidad o utilizando una falsa, intervenga en entornos o plataformas digitales con la finalidad de identificar a los autores o partícipes de un delito, impedir su consumación o reunir información y elementos de prueba necesarios para la investigación.

Esta técnica especial de investigación y prueba procederá para los delitos previstos en la Ley 23.737 y en los artículos 125, 125 bis, 126, 127, 128, 131 del Código Penal, y para delitos cuya pena máxima en abstracto sea superior a tres (3) años de prisión.

La autorización se tramitará conforme a lo regulado en el artículo 204 bis de este código, y deberá acreditarse alguno de los siguientes supuestos:

a) Que el éxito de la investigación resulte seriamente dificultado de no recurrirse a esta técnica;

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

La actuación encubierta no podrá exceder del plazo de noventa (90) días, prorrogable fundadamente por idéntico término y por única vez por auto fundado, a contar desde que la autorización otorgada por el Juez sea notificada al Fiscal.

Podrá autorizarse la obtención de imágenes y la grabación de conversaciones que el agente encubierto mantuviere con otros sujetos.

Librada la autorización judicial, la designación del agente encubierto informático y la instrumentación necesaria para su actuación estará a cargo del Ministerio de Justicia y Seguridad o el organismo que en un futuro lo reemplace, que actuará en enlace permanente con la Fiscalía.

Los perfiles o identidades digitales no podrán emplear imágenes de personas reales y serán creados y administrados por funcionarios de las fuerzas de seguridad, de investigación judicial o de organismos de inteligencia designados a tal fin.

La medida será registrada mediante cualquier medio técnico idóneo que permita la valoración de la información obtenida, debiendo resguardarse su inalterabilidad y la cadena de custodia. Deberá consignarse la denominación y las características del perfil utilizado por el agente encubierto, la plataforma digital en donde actúa, las

claves de acceso validadas y la actividad concreta desarrollada por el agente con la finalidad de identificar autores o partícipes, impedir la consumación de un delito y reunir información y elementos de prueba necesarios para la investigación.

El agente encubierto informático podrá intercambiar o enviar archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos. No se ejercerá acción penal contra el agente que incurriere en un delito como consecuencia necesaria del desarrollo de la actuación encomendada, siempre que esta 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. Si el agente encubierto informático resultare imputado en un proceso, hará saber confidencialmente su carácter a la Fiscalía o al juez, quienes, de forma reservada, recabarán la pertinente información de la autoridad correspondiente. Verificada la calidad en cuestión, se resolverá sin develar la verdadera identidad del agente.

Para los funcionarios encargados de efectuar la intervención y el resguardo rige el deber de confidencialidad y secreto respecto de la información obtenida por estos medios, excepto respecto de la autoridad que la haya requerido. Quienes incumplan este deber incurrirán en responsabilidad personal. El Tribunal dispondrá por auto fundado, a pedido de la Fiscalía, la destrucción ante la presencia de al menos dos (2) testigos del material registrado que no tenga vinculación con la causa."

Artículo 4°: Incorpórese el Capítulo VII, bajo la denominación de "Registros de dispositivos electrónicos, digitales e informáticos", al

Título II "Prueba", del Libro II "Actividad Procesal" del Código Procesal Penal de la Provincia de Santa Fe, el que quedará redactado de la siguiente manera:

"Capítulo VII.- Registro de dispositivos electrónicos, digitales e informáticos.

Artículo 204 Novies – Registro físico de dispositivos electrónicos, digitales e informáticos.- Cuando se hubieren secuestrado dispositivos electrónicos, tecnológicos o cualquier otro susceptible de almacenamiento digital de información, y existieran motivos suficientes para razonablemente presumir que en ellos o en sus sistemas informáticos existe evidencia digital respecto del hecho investigado, el Juez, a solicitud del fiscal, ordenará mediante auto fundado el acceso a dichos dispositivos. El acceso se ordenará al fin de recabar los datos informáticos allí contenidos y de realizar una copia forense del mismo. El auto del Juez deberá fijar los términos y el alcance de los datos que se recabarán y almacenarán, no pudiendo alcanzar a aquellos ajenos a los hechos de cuya investigación se trata y preservando la intimidad y privacidad del tenedor de dichos datos.

Si del registro del dispositivo o su sistema de información, surgieran motivos suficientes para considerar que la evidencia buscada se encuentre total o parcialmente almacenada en otros dispositivos electrónicos, digitales o informáticos situado dentro del territorio nacional y se pudiera acceder a ellos por medio del sistema inicial o estuvieren disponibles para éste, el Juez deberá previamente y a pedido del Fiscal actuante, autorizar dicha requisa, a menos que lo hubiera sido ya en el auto inicial de registro.-"

Artículo 5°: Incorpórese el Artículo 204 Decies al Código Procesal Penal de la Provincia de Santa Fe, el que llevará la siguiente redacción:

"Artículo 204 Decies – Registro remoto de dispositivos electrónicos, informáticos y digitales.-

1. El Juez, a pedido del Fiscal podrá ordenar por auto fundado el registro remoto de dispositivos electrónicos, informáticos o digitales que no se encontraren secuestrados mediante la instalación de un software que permita el examen a distancia de los datos a recabar, siempre que hubiere motivos suficientes que razonablemente hagan presumir la existencia de éstos y su vinculación con el hecho que se investiga.

Este registro procederá en los siguientes supuestos:

a) En casos urgentes en los que estuviera en riesgo inminente la vida, libertad o integridad física o sexual de las personas;

b) Cuando exista riesgo inminente de pérdida de evidencia o elementos probatorios y la requisa remota sea la única forma de evitar dicho riesgo;

c) En todos los casos de investigación de los delitos previstos en los artículos 125, 125 bis, 126, 127, 128, 131, 145, 145 bis, 145 ter, 146, 147 y 170 del Código Penal.-

2. La autorización deberá determinar las condiciones de ejecución de la medida, la que no podrá tener una duración de más de treinta (30) días, pororrogable por igual período hasta un máximo de 90 (noventa) días.-

La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos,

datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida;

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información;

c) Los agentes autorizados para la ejecución de la medida;

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos;

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

Si del registro del dispositivo o su sistema de información, surgieran motivos suficientes para considerar que la evidencia

buscada se encuentre total o parcialmente almacenada en otros dispositivos electrónicos, digitales o informáticos situado dentro del territorio nacional y se pudiera acceder a ellos por medio del sistema inicial o estuvieren disponibles para éste, el Juez deberá previamente y a pedido del Fiscal actuante, autorizar dicha requisa, a menos que lo hubiera sido ya en el auto inicial de registro.-"

Artículo 6°: Modifíquese el Artículo 240 del Código Procesal Penal de la Provincia de Santa Fe, el que quedará redactado de la siguiente manera:

"Artículo 240.- Secuestro. El Fiscal podrá disponer en caso de urgencia, el secuestro de aquellas cosas relacionadas con el delito, las sujetas a decomiso o las que puedan servir como prueba. En todos los procesos por amenazas, violencia familiar o de género, o en cualquier otro delito derivado de situaciones de conflictos interpersonales, el Fiscal deberá disponer el secuestro de las cosas utilizadas en el hecho, como así también aquellas armas de fuego de las cuales el denunciado fuera el tenedor o poseedor, o según las constancias de la causa se hallen en su poder.
Si mediare peligro en la demora, la medida podrá ser cumplida por la policía, que deberá dar aviso sin dilación alguna al Fiscal. Se elaborará un acta de la diligencia de acuerdo a las normas generales.
Las cosas recogidas serán identificadas y conservadas bajo sello, debiéndose adoptar en todo momento las medidas necesarias para evitar alteración. También podrá disponerse la conservación y copia de datos informáticos o evidencia almacenada en dispositivos electrónicos, informáticos y digitales, determinándose la

inaccesibilidad a los mismos hasta el momento de la actuación pericial, excepto en casos urgentes.
Todo aquel que tenga en su poder objetos o documentos que puedan servir como medios de prueba, estará obligado a presentarlos y entregarlos cuando le sean requeridos, siendo de aplicación las medidas de coacción permitidas para el testigo que se rehúsa declarar. Si los objetos requeridos no son entregados, se dispondrá su secuestro. Quedan exceptuadas de esta disposición las personas que puedan abstenerse de declarar como testigos.
Con autorización del Fiscal, o en su caso del Tribunal, los interesados o quienes aquellas autoridades dispongan, podrán tener acceso a las cosas secuestradas, a fin de reconocerlas o someterlas a pericia.
Se llevará un registro en el que conste la identificación de las personas autorizadas.
Serán de aplicación para el secuestro las normas previstas para la requisa y el registro."

Artículo 7°: Incorpórese el Artículo 240 Bis "Orden de Conservación Rápida de Datos Informáticos Almacenados" al Código Procesal Penal de la Provincia de Santa Fe, el que llevará la siguiente redacción:
"Artículo 240 Bis. Orden de conservación rápida de datos informáticos almacenados. Cuando existan motivos suficientes para razonablemente asumir que ciertos datos informáticos pueden ser susceptibles de pérdida, modificación o adulteración, el Fiscal podrá solicitar al Juez, que éste ordene a personas físicas o jurídicas la conservación rápida y la protección de la integridad de datos informáticos específicos de un usuario o abonado que obren en su

poder o bajo su control. La orden será librada por el Juez mediante auto fundado, especificando los datos concretos que se pretende conservar y la duración de la medida que no podrá exceder de ciento veinte (120) días, prorrogables por igual período si se mantuvieren los motivos que fundamentaron la orden.

A su vez, podrá disponer la misma medida respecto de toda persona física o jurídica que preste un servicio de comunicaciones o a los proveedores de Internet de cualquier clase la entrega de datos personales o de identificación de los usuarios y abonados u otra información asociada, que tengan bajo su poder o control.

La orden podrá contener la indicación de que la medida deberá mantenerse secreta y el destinatario estará obligado a adoptar las medidas técnicas de seguridad a estos efectos."

Artículo 8°: Comuníquese al Poder Ejecutivo.-

AUTORES: PERALTA, EMILIANO – AZANZA, ALICIA
Diputados Provinciales

FIRMANTES:
BROUWER, BEATRIZ (Somos Vida)
GRANATA, AMALIA (Somos Vida)
MALFESI, SILVIA (Somos Vida)
PAREDES, OMAR (Somos Vida)
PORFIRI, EDGARDO (Somos Vida)
ROSÚA, MARTÍN (UCR – Unidos para Cambiar Santa Fe)
GONZÁLEZ, MARCELO (UCR – Unidos para Cambiar Santa Fe)
DISTEFANO, SILVANA (UCR – Unidos para Cambiar Santa Fe)

RABBIA, MIGUEL ELÍAS (Juntos Avancemos)

DE PONTI, LUCILA (Juntos Avancemos)

FUNDAMENTOS

Señora Presidenta:

En el año 2001 en la ciudad de Budapest, Hungría, fue firmado por cuarenta y cinco de los cuarenta y siete Estados miembros del Consejo de Europa el "Convenio sobre la Ciberdelincuencia" (Serie de Tratados Europeos N° 185). De esos 47 estados miembros, 35 lo han ratificado y forman ya, entonces, parte operativa de su ordenamiento jurídico y en plena vigencia desde el año 2004.-

Muchos otros países no pertenecientes al Consejo de Europa han sido invitados a adherir al Convenio en cuestión, y otros han firmado y ratificado este instrumento siendo entonces partes integrantes de la convención.

Este Conviene establece en su preámbulo, algunos objetivos, entre los cuales se encuentra *"la necesidad de aplicar, con carácter prioritario una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional"* a partir de una situación que no ha perdido vigencia al día de hoy: la preocupación *"por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes"*.

Esta *política penal común* implica tanto la legislación penal sustantiva (*"de fondo"*) como la procesal (*"de forma"*); ello, con el

fin de prevenir los actos que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos, así como la protección de legítimos intereses, muchas veces víctimas de abusos de dichos sistemas, redes y datos.

Por supuesto, todas estas acciones deben enmarcarse en el marco de los derechos humanos fundamentales como son la intimidad y la privacidad que pueden verse vulnerados en este tipo de procedimientos. El Convenio de Budapest que aludimos y citamos, busca garantizar este equilibrio.

Nuestro país, en aras al cumplimiento de estos objetivos, aprobó por ley del Congreso Nacional el 15 de Diciembre de 2017 el "Convenio de Budapest sobre la Ciberdelincuencia" (Ley N° 27.411). En Latinoamérica también lo ha aprobado el Congreso Colombiano en Julio de 2018.-

En materia de legislación sustantiva (*"de fondo"*), nuestro país ya había aprobado en Junio de 2008 la Ley N° 26.388, denominada "Ley de Delitos Informáticos", modificatoria del Código Penal Argentino, mediante la cual se tipifican distintas figuras delictivas de los "ciberdelitos", tales como la ciber pornografía intanfil, el 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 personales, las defraudaciones informáticas, entre otras.

Ya en el año 2013, se sancionó la Ley de Grooming, bajo el N° 26.904, que tipificó el delito de abuso sexual digital perpetrado contra personas menores de edad realizado a través de comunicaciones electrónicas.

Finalmente, en Marzo de 2018, el Congreso nacional aprobó la Ley N° 27.436, que penaliza al que *"...produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores."*

Sin embargo, más allá de todos estos avances en materia de derecho penal sustantivo, poco se ha progresado en la regulación procesal de la materia en las distintas jurisdicciones de la República Argentina, circunstancia de la que no es ajena nuestra Provincia de Santa Fe. Sólo Salta, Córdoba y Mendoza -en alguna medida- han avanzado en materia procesal (de hecho, algunas de las modificaciones que aquí se proponen han sido tomadas de la legislación de las antedichas provincias y de ante proyectos que no fueron -aún- aprobados). Sí se han incorporado algunas novedades al Código Procesal Penal Federal, de novísima aplicación en nuestra Provincia, que reflejan también institutos del derecho comparado (principalmente, de la Ley de Enjuiciamiento Criminal de España).

Volviendo a Santa Fe, el establecimiento del sistema procesal penal de corte acusatorio adversarial busca -entre otras cuestiones- que en la etapa de investigación penal preparatoria (IPP) se recolecten todas las evidencias que serán luego ofrecidas como pruebas para ser producidas en el juicio oral y público ulterior, única etapa en la que el Juez de juicio (o, en su caso, el Jurado) conocerá la prueba ofrecida en la etapa intermedia del

proceso penal y que luego podrán alcanzar el valor de prueba para que ese juzgador (o, en su caso, el jurado) pueda dar sustento a su sentencia. Y en ello, en el ámbito del mundo de la ciber criminalidad, es menester que las herramientas de recopilación de pruebas respeten los estándares de derechos humanos de las garantías del bloque de constitucionalidad -para evitar luego exclusiones probatorias- pero que también permitan el legítimo ejercicio del poder punitivo del estado.

En nuestra provincia, el actual Defensor del Pueblo Jorge Henn, presentó -cuando Diputado- un proyecto por el cual se incorporaba al Código Procesal Penal de Santa Fe la medida del registro remoto de dispositivos digitales. En su propuesta, se incorporaba como Artículo 170 Bis el "allanamiento remoto de dispositivos tecnológicos", tal consta en el Expte. N° 36.972 de su autoría, y del cual también nos hemos servido para la redacción del presente.-

Vale destacar, entonces, que este proyecto abordará las normas procesales que se aplicarán a la investigación de, por un lado, delitos *"tradicionales"* o *"comunes"* que dejan rastro digital o que se perpetúan a través de medios o plataformas digitales (tales como una estafa, defraudación o extorsión) como aquellos que son verdaderos *ciberdelitos*, como el *"phishing"* (o suplantación de identidad), el *"grooming"* (ya descripto), la *"sextorsión"* (o extorsión a partir de la tenencia de fotografías íntimas de contenido sexual), la pornografía infantil digital, etc.

Una de las dificultades que plantea la temática aquí abordada está dado por la evolución continua de la tecnología informática y de las comunicaciones. Con lo cual, el presente proyecto es punta

de lanza para las modificaciones que son necesarias al día de hoy pero que, por supuesto, en el futuro deberán ser complementadas.

Antes de adentrarme, entonces, en la reforma propuesta, haremos saber que además de la producción intelectual propia, me he servido de legislación comparada como la Mendocina, el Código Procesal Penal Federal y la Ley de Enjuiciamiento Criminal del Reino de España. También, han aportado en cantidad y calidad los Dres. Agustín y Andrés Genera, de Rosario y el Dr. Juan Pablo Malberti, miembro del Ministerio Público de la Acusación de la Provincia de Santa Fe, 4ta Circunscripción.

Siendo entonces que el dictado de los códigos procesales constituye materia de las facultades NO delegadas en el Congreso de la Nación, esta Legislatura se encuentra facultada y legitimada para el dictado de la presente norma que se propone.

Si bien nuestro Código Procesal Penal establece en su artículo 159 el principio de libertad probatoria *("Todos los hechos y circunstancias relacionados con el objeto del proceso podrán ser acreditados por cualquier medio de prueba, salvo las excepciones previstas por las leyes...")*, éste debe ser interpretado a la luz de la máxima *nulla coactio sine lege*[1], 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 limita la interpretación extensiva y la analogía en tanto éstas no favorezcan la libertad del imputado ni el ejercicio de las facultades antes referidas. Ello, toda vez que la interpretación analógica de las normas quedaría sujeta a la

[1] https://adc.org.ar/wp-content/uploads/2019/06/032-evidencia-igital-investigacion-de-cibercrimen-y-garantias-del-proceso-penal-jornada-de-trabajo-12-2017.pdf

aplicación de los operadores de justicia en materia de prueba, lo que impide la existencia de estándares generalizados en la judicialidad relativos a la motivación, proporcionalidad y legalidad de la medida tendiente a recabar, tratar y valorar la prueba digital.

Colorario de esto, y tal lo expresado por la Comisión Interamericana de Derechos Humanos en el Informe 38/96[2], si una medida afecta derechos protegidos en la Convención Interamericana de Derechos Humanos, ésta debe estar necesariamente prevista por la ley, lo que es ni más ni menos que la concreción de la máxima *nulla coactio sine lege*. Es por ello que existe la necesidad de regular estos instrumentos de prueba que, si bien en día hoy se aplican, no tienen regulación específica.

Dicho de otro modo, la relevancia del proyecto está dada en la importancia de que toda la incorporación de prueba al procedimiento sea legal, pues su la misma ha sido recabada en detrimento de garantías y derechos constitucionales(y vaya que aquí se está avanzando sobre derechos y garantías fundamentales como la intimidad y privacidad de las personas), la misma estará viciada y echará por tierra toda la investigación y el proceso.

Comenzaremos, ahora sí, con el análisis específico de cada reforma propuesta.-

1. La primera de las modificaciones tiene que ver con el Artículo 169 del Código Procesal Penal de Santa Fe (en adelante, CPP) en donde se prevé expresamente que cuando en el marco de un allanamiento se encontraren dispositivos tecnológicos, por norma general se prohíbe el acceso a los datos y contenidos de los

[2] https://defensoria.org.ar/normativas-cdh/comision-interamericana-de-derechos-humanos-informe-n-38-96/

mismos. Ello, en preserva de las garantías y derechos constitucionales de los investigados. Esta regla, por supuesto, admite excepción, que es la autorización del Juez "según las disposiciones de este Código". Y es que el ordenamiento jurídico prevé circunstancias excepcionales donde sí podría autorizarse (las analizaremos después, además de las situaciones ya previstas en la legislación actual); pero además, si la orden de allanamiento ya prevé esta posibilidad, pues podrá accederse a los mismos. En caso contrario, el fiscal de la causa habrá de solicitar la autorización judicial para el acceso correspondiente.

2. Seguidamente, se modifica el Artículo 171 del CPP. En la reacción vigente, este artículo -que versa sobre la interceptación de correspondencia e intervención de comunicaciones- ya comprende los intercambios de correspondencia "electrónica", pero la regulación es por demás escueta y no se adapta a los estándares internacionales en la materia. Es que la intercepción de estas comunicaciones es tan intrusiva en la vida de las personas, afectando datos básicos, de tráfico y de contenido (tal la clasificación del Convenio de Budapest, estos últimos contienen datos de injerencia en la vida privada y el acceso a la información más íntima y sensible de la persona intervenida), que requerirá distintos grados de convicción del Juez al momento de ordenarla y ciertamente un período de tiempo por el cual las mismas pueden ser ordenadas.

Para la modificación propuesta se tomó como modelo la disposición del novel Código Procesal Penal Federal en su artículo 150 y varias disposiciones de la Ley de Enjuiciamiento Criminal del Reino de España (Capítulos IV, V y VI de la misma).

Se establece expresamente que la intervención de la comunicación digital será de carácter excepcional (ya que requiere el más alto grado de convicción judicial para ordenarla, según los estándares del Convenio de Budapest) y tiene un límite de duración: treinta (30) días, plazo que podrá ser renovado sólo mediante resolución fundada y siempre que existieran causas que así lo justifiquen, indicándose el nuevo plazo de renovación. En el Código Procesal Penal Federal no existe pauta de límite de renovación. La Ley Española establece sí, como máximo, dieciocho meses. Entendemos que la solución del Código Federal se ajusta a nuestro sistema y que, en definitiva, los casos en que se lleguen a dieciocho meses de intervención de comunicaciones serán casi inexistentes, atento a que la medida ha de ser debidamente fundada por el Juez que ordena y resulta dificultoso pensar que razonablemente un juez crea que, después de varios meses de intercepción de comunicaciones sin éxito, pueda decidir mantener la medida o que, por el contrario, con la cantidad de evidencia que se puede recolectar en ese plazo, no haya aún preparado el fiscal la acusación sin caer en algún supuesto de mal desempeño por mora en su tarea.

Por supuesto que rige para los intervinientes en la medida, el deber de confidencialidad y secreto de la información obtenida, so pena de responsabilidad penal. Por otra parte, rige el deber de colaboración para las empresas que brindan este servicio de comunicación, bajo apercibimiento de mismas sanciones.

Importante es destacar que se incorporan las causales de cesación de la medida: desaparición de las circunstancias que justifican la medida, agotamiento del plazo de la misma,

cumplimiento del objeto o imposibilidad de cumplir con el objeto de la misma. En todos los casos, se interrumpirá inmediatamente la medida.-

3. Con la última reforma al Código Procesal Penal de Santa Fe, dispuesta por Ley N° 14.258, se incorporó el Capítulo VI al Título II del Libro II del Código ritual, bajo la denominación de "Técnicas Especiales de Investigación y Prueba". Allí se incorporan figuras como las del agente encubierto, agente revelador, informante y arrepentido.

Proponemos en esta reforma incorporar lo que se conoce como *"agente encubierto informático"*, a través de lo que será el artículo 204 Octies. Para la redacción del presente, se tomó como antecedente normativo uno de los proyectos de reforma de la Provincia de Mendoza, pero también las disposiciones del Artículo 282 bis, incisos 6 y 7 de la Ley de Enjuiciamiento Criminal de España.

Se busca con este instituto incorporar la figura del agente encubierto a un ámbito muy particular como es el de la cibercriminalidad.

Al igual que el agente encubierto ya incorporado al CPP por la reforma de la ley N° 14.258, esta técnica especial de investigación y prueba procederá para los delitos previstos en la Ley 23.737 y en los artículos 125, 125 bis, 126, 127, 128, 131 del Código Penal, y para delitos cuya pena máxima en abstracto sea superior a tres (3) años de prisión, tal la previsión del artículo 204 bis, al que también remitimos respecto en la forma de tramitación de la petición.

Se agregan, sí, que la medida se dispondrá siempre que el éxito de la investigación esté seriamente comprometido en caso de no recurrirse a esta técnica (es decir, el criterio de aplicación es restrictivo) ó bien que se trate de delitos cometidos a través de medios informáticos que no permitan otra forma de investigación. Son distintos supuestos y basta que se dé uno u otro (es decir, no son acumulativos).

La finalidad de este medio particular de investigación y prueba es que el agente encubierto informático, ocultando su identidad o utilizando una falsa, intervenga en entornos o plataformas digitales a fin de identificar a los autores o partícipes de un delito, impedir su consumación o reunir información y elementos de prueba necesarios.

Se fija también un plazo máximo de actuación (90) días que sólo puede ser renovado por otro plazo igual y por única vez, bajo resolución fundada. Se establece en el articulado también una serie de pautas en relación a la responsabilidad del agente encubierto en caso de cometer ilícitos en el desarrollo de su accionar; también los deberes de secreto y confidencialidad y la posibilidad de destrucción de los elementos recolectados durante la investigación una vez terminado el proceso penal.

4. En lo que hace al registro de dispositivos electrónicos, digitales e informáticos, se puede efectuar de dos maneras: registro físico (esto es, cuando surge de un secuestro en el marco de un allanamiento) o registro remoto (este es el que se hace sin necesidad de previo secuestro del dispositivo). Incorporamos en la norma ambos supuestos, a través de la incorporación del Capítulo VII "Registros de dispositivos electrónicos, digitales e informáticos"

al Título II de "Prueba" del Libro II "Actividad Procesal" del Código Procesal Penal.

Serán los artículos 204 Novies y Decies los que reglarán los registros físicos y remotos, respectivamente.

El artículo 204 Novies propuesto permite que el juez, a solicitud del fiscal y por resolución fundada, ordene el acceso a dispositivos secuestrados a fin de recabar datos contenidos en el mismo y realizar (de ser necesario) una copia forense y de extender la requisa incluso a otros dispositivos dentro del territorio nacional que pudieran ser accesibles vía remota a través del dispositivo periciado.-

El artículo 204 Decies permite el registro de estos mismos dispositivos, pero de manera remota. Dado que la intromisión en la intimidad de la persona es quizás de máxima hipótesis con esta medida, la misma será de carácter restringido y procederá solamente en alguno de los siguientes casos: a) riesgo inminente para la vida, libertad o integridad física o sexual de las personas (recalcamos la inminencia del riesgo), b) peligro inminente de pérdida de evidencia o elementos probatorios y (requisito acumulativo) que la requisa remota sea la única forma de evitar ese riesgo; c) En los casos en que se investiguen los delitos previstos por el Código Penal en los artículos 125, 125 bis, 127, 128, 145, 145 bis, 145 ter, 146, 147 y 170 de la norma nacional.

La medida tiene un plazo de duración máxima de treinta (30) días, prorrogable por igual período hasta un máximo de noventa (90) días. Se tomó, para ello, el criterio de la Ley de Enjuiciamiento Criminal de España (Art. 588 septies, inciso c), que establece este

plazo en meses (convirtiéndolo en plazos de días, en armonía con el resto de las disposiciones de nuestro Código Procesal Penal.-

5. En relación al secuestro (medida de coerción real prevista en el artículo 240 del CPP), proponemos modificar dentro del artículo el párrafo siguiente (la modificación se establece en negrita): *"Las cosas recogidas serán identificadas y conservadas bajo sello, debiéndose adoptar en todo momento las medidas necesarias para evitar alteración.* ***También podrá disponerse la conservación y copia de datos informáticos o evidencia almacenada en dispositivos electrónicos, informáticos y digitales, determinándose la inaccesibilidad a los mismos hasta el momento de la actuación pericial, excepto en casos urgentes"***. Ello va en línea con la modificación propuesta al Artículo 169 en relación al allanamiento y constituye una garantía en favor del imputado.

6. Por último, se propone incorporar seguidamente a este artículo, una nueva disposición (Artículo 240 Bis) relativo a la *"Orden de conservación rápida de datos informáticos almacenados"*. La medida procede cuando estos datos puedan ser susceptibles de pérdida, modificación o adulteración. El Juez se lo ordenará a personas físicas o jurídicas la conservación de estos datos que sean de sus usuarios o abonados. La medidas se puede ordenar por el plazo de ciento veinte (120) días, prorrogable por igual período con debidos fundamentos (el plazo surge, en parte, de lo previsto en la Ley de Enjuiciamiento Criminal Española).

Creemos, Sra. Presidenta, que este proyecto es un puntapié inicial para la modernización de nuestro código ritual en materia

penal y que comienza a ponerse a tono con las legislaciones más avanzadas en la materia. En un mundo en que las manifestaciones del delito han adquirido matices o medios quizás hasta el momento desconocidos, resulta fundamental con las herramientas necesarias para la investigación de los hechos con apariencia de ilícito penal. Seguramente con la constante evolución de la tecnología, se necesitarán ulteriores reformas a la aquí presentada.

Por otra parte, entendemos también que se ha propuesto una reforma que conjuga las necesidades punitivas y de persecución del delito del estado, con las garantías y derechos previstos en la constitución y en los tratados internacionales de derechos humanos, en la preservación de la esfera de intimidad y preservación de las personas.

Es por ello, Sra. Presidenta, que solicitamos a nuestros pares el acompañamiento y aprobación del presente proyecto de ley.-

EMILIANO JOSÉ PERALTA
Diputado Provincial

ALICIA AZANZA
Diputada Provincial

AMALIA GRANATA
Diputada Provincial

FIRMANTES:
BROUWER, BEATRIZ (Somos Vida)
GRANATA, AMALIA (Somos Vida)

MALFESI, SILVIA (Somos Vida)

PAREDES, OMAR (Somos Vida)

PORFIRI, EDGARDO (Somos Vida)

ROSÚA, MARTÍN (UCR – Unidos para Cambiar Santa Fe)

GONZÁLEZ, MARCELO (UCR – Unidos para Cambiar Santa Fe)

DISTEFANO, SILVANA (UCR – Unidos para Cambiar Santa Fe)

RABBIA, MIGUEL ELÍAS (Juntos Avancemos)

DE PONTI, LUCILA (Juntos Avancemos)