INCORPORACIÓN DE LA EVIDENCIA DIGITAL AL CÓDIGO PROCESAL PENAL DE LA PROVINCIA DE SALTA

JOSE ARÁOZ FLEMING
SALTA

INCORPORACIÓN DE LA EVIDENCIA DIGITAL AL CÓDIGO PROCESAL PENAL DE LA PROVINCIA DE SALTA

RESUMEN

Se encuentra en avanzado estado de tratamiento en la Cámara de Senadores de la Provincia de Salta y cuenta con media sanción de su Cámara de Diputados, un proyecto de modificación del Código Procesal Penal que fundamentalmente apunta a la incorporación de la evidencia digital a su articulado.

Este proyecto tuvo sus inicios en el mes de marzo del año 2021, cuando el entonces procurador de la provincia, Dr. Abel Cornejo, creo la comisión de reforma del Código Procesal Penal de Salta; "… para el análisis del **tratamiento de la evidencia digital** en la actualidad y proyección de una futura reforma…".

Quien suscribe tuvo el honor de ser invitado a integrar dicha Comisión en representación del Colegio de Abogados y Procuradores de Salta, junto a los Dres. Diego Perez, ex Secretario de Justicia de la Provincia, Sofia Cornejo, hoy fiscal del ciberdelito de nuestra provincia, el Dr. Marcos Salt y representantes de las Universidades entre otros. Asimismo, la Universidad Católica de Salta, por medio de su IDeNTec lleva adelante un proyecto de investigación al respecto.

En la antesala del proyecto, al abordar figuras tales como la del agente encubierto digital, la posibilidad de obtención remota de datos, la intervención de todo tipo de comunicaciones; nuestra postura siempre fue la del respeto irrestricto de las garantías constitucionales, de garantías individuales tales como la privacidad, la intimidad, etc.; entendiendo, obviamente, que las herramientas que la reforma hoy propone son fundamentales a los fines de encarar los nuevos tiempos de la delincuencia organizada.

CONCLUSIONES

El avance tecnológico aplicado al delito requiere soluciones análogas y estas demandan obviamente reformas de nuestros vetustos Códigos Procesales; añejos no por falta de conocimientos o de idoneidad de sus redactores sino simple y sencillamente porque lo que hoy tenemos, en su época, no existía, porque los tiempos cambian. Lo que hoy nos abruma, y a veces hasta nos avasalla, hace algunos años lo veíamos solo en las películas de ciencia ficción.

En la investigación penal, la evidencia física lo era todo. Hoy la evidencia digital prácticamente está presente en todos los delitos; no necesariamente como actor principal o como factor fundamental de su consumación (caso grooming) sino en delitos de cualquier tipo como un homicidio, por citar solo un ejemplo. El conocer por donde transitó el celular de la víctima, o del posible imputado, o cual fue el camino que siguió ese móvil, nos permite arribar a un alto grado de certeza en las investigaciones, nos permite descubrir crímenes que hubiesen quedado impunes en otros tiempos. ¿Cómo lo hacemos? Con la triangulación de las antenas de telefonía móvil, con lo informes de las compañías telefónicas, con la información existente en el propio aparato de la víctima o el autor del delito.

¿Cómo obtenemos esta evidencia? Con el aseguramiento de los siempre volátiles datos informáticos. Con la posibilidad de obtenerlos de parte de las empresas proveedoras de servicios. Con la posibilidad de secuestrarlos, de obtenerlos remotamente, de introducir los agentes encubiertos digitales en el entorno virtual, en la red investigada, entre otras herramientas.

INCORPORACIÓN DE LA EVIDENCIA DIGITAL AL CÓDIGO PROCESAL PENAL DE LA PROVINCIA DE SALTA

Se encuentra en avanzado estado de tratamiento, en la Cámara de Senadores de la Provincia de Salta, y cuenta con media sanción de su Cámara de Diputados, un proyecto de modificación del Código Procesal Penal que, fundamentalmente, apunta a la incorporación de la evidencia digital a su articulado.

Este proyecto tuvo sus inicios en el mes de marzo del año 2021, cuando el entonces procurador de la provincia, Dr. Abel Cornejo, creo la comisión de reforma del Código Procesal Penal de Salta; "… para el análisis del **tratamiento de la evidencia digital** en la actualidad y proyección de una futura reforma…".

Quien suscribe tuvo el honor de ser invitado a integrar dicha Comisión en representación del Colegio de Abogados y Procuradores de Salta, junto a los Dres. Diego Pérez, ex Secretario de Justicia de la Provincia, Sofia Cornejo, hoy fiscal del ciberdelito de nuestra provincia, el Dr. Marcos Salt y representantes de las Universidades entre otros. Asimismo, la UCASAL (Universidad Católica de Salta), por medio de su IDeNTec (Instituto de Derecho de las Nuevas Tecnologías) lleva adelante un proyecto de investigación al respecto.

DE LA REFORMA EN PARTICULAR.

El proyecto en análisis pretende incorporar al Código Procesal de la Provincia de Salta aprobado por ley provincial 7690 y sus modificatorias, como **Capítulo IV,** los "**Medios de prueba informáticos".**

Como surge de sus considerandos, y, como técnica legislativa, se optó por modificar el actual artículo 309 y agregar los artículos desde el 309 bis al 309 sexies, y, de este modo evitar, tener que modificar la numeración de todo el articulado.

El proyecto quedó estructurado de esta manera: Art. 309 - Principios generales; Art. 309 bis - Aseguramiento de datos; Art. 309 ter - Orden de presentación de datos informáticos; Art. 309 quáter – Obtención de datos informáticos; Art. 309 quinquies – Investigación encubierta en entornos digitales; Art. 309 sexies – obtención remota de datos de dispositivos informáticos.

Asimismo, se modifica el actual artículo 316 vinculado a la interceptación de comunicaciones, incorporando en el título y en el texto, la interceptación de datos de tráfico y de contenido, a las ya existentes: interceptación de correspondencia e intervención de comunicaciones.

El proyecto comienza con una norma de principios generales aplicables a todos los medios de prueba propuestos que resultará fundamental para enmarcar las medidas dentro del esquema de garantías previstos en el texto constitucional y en el CPP. Se aclara la necesidad de que el uso de estos medios se dé en el marco de investigaciones penales concretas evitando los peligros de un uso indiscriminados con finalidades diferentes a las del proceso penal y se acentúa la idea de última ratio en su uso con los principios de necesidad, idoneidad y proporcionalidad.

DE LAS MEDIDAS DE PRUEBA EN PARTICULAR

1. ASEGURAMIENTO DE DATOS: Es una Medida cautelar probatoria que posibilita que al iniciar una investigación se pueda ordenar el aseguramiento de cierta información por determinada cantidad de tiempo; es decir, no se puede ver el contenido del dato, pero sí se asegura que no sea afectado por alteraciones o borrados hasta el momento en que pueda ser pedido judicialmente. Esto se vincula con la volatilidad de los datos; es decir, con este medio de prueba se minimizan casi por completo los riesgos de pérdida de los datos que pueden servir de prueba en una investigación. A modo de ejemplo, en un supuesto determinado de investigación de un fraude acaecido en una plataforma de ventas de comercio electrónico, la posibilidad de pedirle al titular de la empresa de comercio electrónico que asegure determinados datos como los datos de abonados de quien efectuó una venta, logs de conexión, domicilios de entrega de productos, etc. La información no se entregará a quien lleva adelante la investigación, pero se evitaría que sea borrada, por ejemplo, por decisiones de la empresa para evitar los costos del alojamiento de datos. El artículo propuesto como 309 bis establece bajo qué condiciones puede ordenarse la medida, su duración y la obligación de guardar secreto por parte de la persona requerida. Este es un aspecto fundamental ya que, si la persona requerida asegura el dato, pero avisa o difunde de cualquier modo la medida adoptada, puede perjudicar la investigación.

2. ORDEN DE PRESENTACIÓN DE DATOS INFORMATICOS: Si bien esta medida se encuentra regulada en el Código Procesal Penal de Salta, y consiste en poder pedirle a cualquier persona (física o jurídica) que entregue cualquier documentación o cosas que tenga y que esté en su poder., no está pensada para datos informáticos y las características especiales que presenta en su forma y lugar de alojamiento o almacenamiento sino para cosas o documentos físicos. El art. 309 ter pretende solucionar este aspecto. En ambos casos, es una medida previa o menos invasiva que el allanamiento y posterior secuestro. En el caso de la evidencia digital, se puede estar pidiendo a una empresa que entregue cierta información, cierto dato y puede ser que ésta no tenga la disposición de esos datos. Por ejemplo, se puede pedir a un proveedor de servicios en Salta que entregue determinados datos y pueden contestar que los datos están en servidores alojados en otra jurisdicción (en otra provincia, en otro país). Se puede estar pidiendo a un proveedor de servicios que presente o entregue ciertos datos y éstos quizá no están alojados en esa oficina, sino en servidores de extraña jurisdicción. Todas estas situaciones requieren de medidas especiales, las cuales pretende cubrir este proyecto. El articulo proyectado prevé

también la obligación para la persona requerida de mantener bajo reserva la orden recibida.

3. Obtención de datos informáticos **REGISTRO Y SECUESTRO DE DATOS INFORMÁTICOS.** Se incorpora un artículo que regula el registro de un sistema informático o de un medio de almacenamiento de datos informáticos o electrónicos con el fin de obtener los datos allí alojados. Esta medida deberá ser dispuesta por el Juez interviniente, a requerimiento de las partes, y se prevén una serie de medidas y requisitos para garantizar la auditabilidad de las operaciones técnicas que se realicen.

Este artículo se encuentra dividido en varios apartados, entre los cuales se destaca la regulación expresa de los hallazgos casuales, las técnicas de triage y la extensión de registro.

Es innegable que cualquier hallazgo casual debe ser puesto en conocimiento de la autoridad judicial que dio la orden que motivó el registro, a los fines de obtener una nueva

autorización y así evitar nulificar el procedimiento para posibles futuras investigaciones. Y en este sentido que se prevén estas situaciones en el presente proyecto.

Con relación al *triage*, éste viene a acelerar y eficientizar las tareas previas preparatorias para la pericia, y se realizará de tal manera que no se altere el contenido de ninguno de los dispositivos analizados.

Es una técnica que no afecta el derecho de defensa de ningún particular, y puede ser realizada por cualquier personal técnico idóneo, sin necesidad de convocar a peritos informáticos; es una técnica que no reporta mayor dificultad. Es decir, no hay inconveniente en utilizarla si se lo hace como una forma de búsqueda o registro sencillo de datos.

Para garantizar de una mejor manera las garantías de las personas involucradas y no afectar su derecho de defensa, se aconseja trabajar con técnicas de bloqueo de escritura sobre los medios de almacenamiento de información para garantizar que no se altere el contenido del soporte físico que es objeto de análisis, con el fin de garantizar que, frente a cualquier duda o impugnación la medida sea un acto reproducible en términos procesales.

4. INVESTIGACIÓN ENCUBIERTA EN ENTORNOS DIGITALES. AGENTE ENCUBIERTO DIGITAL. Teniendo en cuenta el potente factor de anonimato en que se funda el vasto mundo de internet y la alta cifra negra de delitos no denunciados se genera la necesidad de encontrar medidas de persecución criminal que de alguna u otra forma ayuden a mitigar estos elementos y faciliten la imputación de estas figuras penales informáticas.

Podemos definir al agente encubierto informático como aquel empleado o funcionario público que, de manera voluntaria y por decisión de una autoridad judicial, se infiltra en la red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de ella, mediante la ocultación de su verdadera identidad y con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los ciberdelincuentes actúan, con la finalidad primordial e igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales.

Con la mira en las acciones que pueden llevar a cabo nuestros cuerpos de investigación, podemos trasladar el antiguo agente encubierto a entornos virtuales donde necesariamente debe cambiar ciertos elementos, alterando en parte algunos de sus atributos.

Su activo funcionamiento en el orden procesal penal aparece legitimado por la proporcionalidad de este frente al poder de las organizaciones criminales, así como en

función de los bienes jurídicos que busca proteger. Su existencia tensiona la relación que existe entre el deber del estado de resguardar los derechos fundamentales y la necesidad persecutoria penal de contar con herramientas útiles en el esclarecimiento de los delitos.

El desempeño del agente encubierto, lejos de ser emplazado por las TICs, debe ser asistido por éstas, explotando todas las virtudes de la era moderna para lograr los fines de su acción. Los medios tecnológicos nos permiten estar presentes en el mismo espacio virtual en que los delincuentes digitales actúan, de manera sigilosa y cauta, pudiendo constatar, escuchar y recopilar información más allá de las circunscripciones territoriales, información e indicios que eventualmente pueden utilizarse como elementos de convicción en un proceso penal. De esta forma, se torna en una técnica clave para enfrentar a la criminalidad digitalizada tal como es concebida en la actualidad.

5. OBTENCIÓN REMOTA DE DATOS DE DISPOSITIVOS INFORMÁTICOS.TÉCNICAS DE REMOTE FORENSIC. La utilización por parte del Estado

de programas espías o maliciosos para el registro y secuestro de datos a distancia (técnicas de remote forensic), aparece como un nuevo mecanismo para acceder –subrepticiamente- a la información contenida en soportes informáticos, que no encuadra en ninguna de las normas que prevén los medios de prueba tradicionales, es decir que se trata de un medio de prueba "híbrido".

No es pacífica la aceptación de estas técnicas como medio de prueba válido; la discusión pasa por la ponderación de dos principios fundamentales en pugna, por un lado, la obligación estatal de investigar y perseguir los delitos y, por el otro, el respeto de la intimidad y privacidad de los ciudadanos (eficiencia vs. garantías).

Pero tal discusión queda zanjada si utilización de este medio de prueba se realiza de manera restrictiva –tal como se lo prevé en este proyecto de reforma-, debiendo hacerse un análisis de la **proporcionalidad**, la **necesidad** y la **razonabilidad** de la medida en cada caso concreto. Además, la medida debe fijarse en un **límite temporal** preciso, debe exigirse **deber de confidencialidad** a los funcionarios estatales que la lleven adelante, a fin de garantizar la intimidad de los resultados que nada tengan que ver con el proceso penal en el que se ordenó.

La utilidad de esta medida está fuera de discusión ante el evidente avance de la tecnología que utilizan los delincuentes en la comisión de los delitos.

6. EQUIPOS CONJUNTOS DE INVESTIGACIÓN E INVESTIGACIONES CONJUNTAS. Se incorpora un artículo que prevé la conformación de equipos conjuntos de trabajo para investigaciones de casos en los que el delito se hubiere cometido y/o tuviere consecuencias, a su vez, en otras jurisdicciones diferentes a la de Salta, es decir en otras provincias.

Estos equipos nacen con el objetivo de mejorar la cooperación interprovincial en las investigaciones de estos delitos y en la recopilación de pruebas en forma electrónica de cualquier delito penal.

La utilidad y necesidad de estos equipos de trabajo está fuera de discusión, por cuanto la actividad delictiva en las redes no conoce de fronteras. Es más, esta modalidad de trabajo conjunto debe extenderse fuera los límites de nuestro país, tal como lo prevé el Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia sobre cooperación y divulgación de evidencia electrónica (Estrasburgo, 12.V.2022).

Se prevé que los procedimientos y condiciones que rijan el funcionamiento de los equipos conjuntos de investigación serán acordados entre las autoridades competentes de las jurisdicciones involucradas y que las pruebas obtenidas por cualquiera de las partes tendrán valor y podrán ser utilizadas por todas ellas en la investigación que motivó la

conformación del equipo.

El avance tecnológico aplicado al delito requiere soluciones análogas y estas demandan obviamente reformas de nuestros vetustos Códigos Procesales; añejos no por falta de conocimientos o de idoneidad de sus redactores sino simple y sencillamente porque lo que hoy tenemos, en su época, no existía, porque los tiempos cambian. Lo que hoy nos abruma, y a veces hasta nos avasalla, hace algunos años lo veíamos solo en las películas de ciencia ficción.

En la investigación penal, la evidencia física lo era todo. Hoy la evidencia digital prácticamente está presente en todos los delitos; no necesariamente como actor principal o como factor fundamental de su consumación (caso grooming) sino en delitos de cualquier tipo como un homicidio, por citar solo un ejemplo. El conocer por donde transitó el celular de la víctima, o del posible imputado, o cual fue el camino que siguió ese móvil, nos permite

arribar a un alto grado de certeza en las investigaciones, nos permite descubrir crímenes que hubiesen quedado impunes en otros tiempos. ¿Como lo hacemos? Con la triangulación de las antenas de telefonía móvil, con lo informes de las compañías telefónicas, con la información existente en el propio aparato de la víctima o el autor del delito.

¿Como obtenemos esta evidencia? Con el aseguramiento de los siempre volátiles datos informáticos. Con la posibilidad de obtenerlos de parte de las empresas proveedoras de servicios. Con la posibilidad de secuestrarlos, de obtenerlos remotamente, de introducir los agentes encubiertos digitales en el entorno virtual, en la red investigada, entre otras de las herramientas antes reseñadas y que se pretende incorporar en la reforma.

¿Como evitamos la arbitrariedad del poder frente a la incorporación de estas herramientas? Con los necesarios equilibrios, con el juego de los frenos y contrapesos, poniendo en manos del fiscal la fundamentación de la necesariedad de la medida, dotando al juez de la decisión de su otorgamiento, haciendo andar el engranaje, permitiendo a los que tienen que impulsar la investigación llevarla adelante, sabiendo que quienes tienen que controlarla gozan de todo el poder para ello y, finalmente, activando el eslabón de las responsabilidades para los excesos.

Un sistema de justicia que se precie de ser tal debe contar necesariamente con todos estos engranajes, máxime en nuestra provincia en donde el ministerio público no es parte del poder judicial y justamente el esquema fue diseñado para hacer factible este esquema de frenos y contrapesos.

Así como desde el año 2012 reclamábamos la creación de la fiscalía del ciberdelito en nuestra Provincia y hoy es una realidad, le demos a quienes investigan los delitos las herramientas para hacer posible su función, herramientas idóneas y modernas.

Para el reaseguro, para el control posterior, el poder judicial ya cuenta con las herramientas necesarias, es cuestión de utilizarlas.

Nuestra labor, como abogados, será controlar, activar, estas últimas ante la detección de excesos o de actos reñidos con el fin buscado.