CUESTIONES ACTUALES DE NECESARIO ANÁLISIS

DESAFÍOS LEGALES EN LA ERA DIGITAL

ACTUALIZACIÓN DE TÉCNICAS INVESTIGATIVAS Y EVIDENCIA DIGITAL EN EL MARCO LEGAL ARGENTINO

Autor: Juan Martín Resoagli

Síntesis

El presente artículo examina las técnicas especializadas de investigación y la relevancia de la evidencia digital en el marco de la legislación vigente, focalizándose en la Ley N° 27.319, y una sucinta mención a temas relevante y relacionados que aparecen como novedosas modificaciones introducidas al Código Procesal Penal de Corrientes y en la Ley N° 9.510 de Mendoza.

Se destaca la necesidad de actualizar y adaptar estas regulaciones ante el rápido desarrollo de las tecnologías y la creciente incidencia de delitos cibernéticos. Así también, se resalta la importancia de revisar los criterios de admisión y tratamiento de la evidencia digital en los procesos judiciales, así como la urgencia de un enfoque colaborativo entre legisladores, expertos en tecnología y profesionales del derecho para garantizar una regulación efectiva y justa que aborde los desafíos de la era digital.

Introducción

La actualización en materia de investigaciones complejas ha seguido la lógica de incorporar, a la regulación procesal, técnicas especiales para asegurar la prevención, persecución y lucha de este flagelo. Algunos ejemplos de estos modos especiales de investigar aparecen contenidas en la Ley N° 27.319. Pero este tipo de investigaciones no se limita a las grandes organizaciones que funcionan en nuestro país, sino que también termina alcanzando a delincuentes que desde el anonimato y la independencia causan estragos.

En este sentido, esta ley del año 2.016 ha quedado desactualizada y en gran medida esto se ha debido al *boom* que han generado las nuevas tecnologías de los sistemas informáticos como herramientas para cometer delitos. Esta nueva realidad ha suscitado importantes debates en torno a la evidencia digital, su admisión y los requisitos que debe cumplir, lo cual ha provocado la evolución de ciertas legislaciones procesales en el país. No obstante, queda evidente que aún queda un considerable trabajo por realizar en este ámbito.

En este complejo escenario, resulta imperativo abordar tanto la actualización de las técnicas especializadas de investigación contempladas en la legislación vigente como la modificación de las normativas procesales relacionadas con las investigaciones en el ciberespacio y las referidas a la evidencia digital. Este debate se ve agravado por la ampliación del espectro de lo que se consideraba un delito

complejo hace algunos años, una evolución que aún no se ha reflejado de manera adecuada en la legislación.

El propósito de este artículo es analizar las implicaciones de las técnicas especiales de investigación y, el rol que ocupa la evidencia digital en ellas, según la legislación actualmente vigente. Además, se busca realizar una comparación con regímenes más modernos, evaluando la necesidad de seguir sus pasos y actualizar estas técnicas

1. El panorama actual de la ciberdelincuencia

La globalización fue para el siglo pasado un hito a nivel económico y social, y esto se vio reflejado también en como comenzaron a cometerse ciertos delitos. En aquel contexto, la apertura de las fronteras y el ver como "el mundo se hacía más pequeño" potenció que ciertas actividades criminales adquirieran nuevas metas y se materializaran de un modo diferente. Pero la globalización del siglo XIX, y el acelerador que recibió a finales del siglo XX, no fueron el final sino tan solo el umbral para un nuevo universo de modalidades delictivas.

La globalización de la actividad económica, potenciada antes por las mejoras en transporte y fabricación, se vio mejorada aún más con las TICs. Así el internet, las nuevas aplicaciones y la actualización de las plataformas digitales lograron generar un nuevo espacio que los criminales han sabido aprovechar, dando lugar a un nuevo tipo de criminalidad organizada.

En Argentina, este fenómeno de la digitalización de las "mafias", genera un grave problema. El informe del año 2.020 la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) del Ministerio Público Fiscal de la Nación[1], reportaba un aumento de los casos de ciberdelitos comparando los primeros trimestres de los años 2.019, 2.020 y 2.021. En esa oportunidad, los números reflejaban un aumento de reportes en más del 35% para el 2.020 (con un total de 790 con relación a los 581 del período anterior), y de más del 500% si lo comparamos con el primer trimestre de 2.021 (con un total de 3976 reportes recibidos).

Si bien hay que entender que esto se dio en un contexto de pandemia, donde las estadísticas sobre los delitos se vieron alteradas por el contexto de encierro, es menester comprender que muchas de las cosas que la pandemia trajo consigo se

[1] Unidad Fiscal Especializada en Ciberdelincuencia (2021). "Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020". Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). https://www.mpf.gob.ar/ufeci/files/2021/09/UFECI_informe-pandemia.pdf

mantienen a día de hoy, y la ciberdelincuencia es una de ellas. Esto se constata al analizar el informe del año 2.022/2.023 de la UFECI, en el cual se indica que el aumento de delitos en el ámbito digital ha seguido esa tendencia reflejada en el párrafo anterior. El informe señala que entre los meses de abril de 2.021 y marzo de 2.022, se recibieron un total de 25.588 reportes (un 75,5% más que en el periodo anterior), mientras que, entre los meses de abril de 2.022 y marzo de 2.023, se recibieron 35.447 reportes, lo que representa un aumento del 38,5% con respecto al ciclo anterior[2].

En este contexto, los delitos más comunes, de acuerdo a los informes de la UFECI, han sido el fraude en línea (con un aumento del 1782.56% en el período de 2.022 a 2.023, con relación al de 2.019 a 2.020); el acceso ilegítimo (con un incremento del 1124.24%, tomando los mismos períodos); la usurpación de identidad (con un incremento del 56.87% en el período 2.022-2.023 con relación al de 2.021-2.022), entre otros.

Y con estos números solo nos estamos aproximando a la punta del *iceberg* de la ciberdelincuencia. Cuando nos detenemos a analizar estadísticas de otros organismos, es evidente la influencia que la pandemia y el avance de las nuevas tecnologías de la información y la comunicación han tenido y cómo se han convertido en instrumentos para cometer delitos. Así es que por ejemplo,en el año 2.020 las consultas en relación al delito de grooming aumentaron un 133% respecto al mismo período del año 2.019[3].

En este sentido, una crítica común de los informáticos suele ser que el *software* avanza más rápido que el *hardware*. Pues, aunque no siempre se lo mencione, uno de los problemas para los operadores del derecho y las fuerzas de seguridad suele ser que las herramientas de los delincuentes suelen avanzar de forma más rápida que las propias de estos grupos que se encuentran “del lado de la ley”, por englobarlos de algún modo. En otras palabras, es manifiesto que las formas en que se comenten los delitos se actualizan más rápido que las herramientas para perseguirlos.

---

[2] Unidad Fiscal Especializada en Ciberdelincuencia (2023). “Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022-2023”. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). https://www.fiscales.gob.ar/wp-content/uploads/2023/12/UFECI_informe-de-Gestion_23_15-12.pdf

[3] Dirección Operativa del Comité Ejecutivo para la lucha contra La Trata de Personas (2019) “Grooming y trata” https://www.argentina.gob.ar/sites/default/files/2019/12/grooming_y_trata.pdf

Esto no es malo en sí mismo, dado que es la propia naturaleza social del derecho la que hace que esta actualización se dé tomando como parámetro las necesidades sociales. Sin embargo, el problema aparece cuando esta renovación en las herramientas no llega oportunamente debido a la falta de acuerdo legislativo y político sobre el asunto.

Es aquí donde los operadores del derecho debemos intervenir para asegurar que los procesos penales de la época actual se mantengan actualizados con las herramientas correctas a fin de garantizar los fines del mismo.

2. La ciber criminalidad organizada, la Ley N° 27.319, las actuales técnicas especiales de investigación y la evidencia digital

2.1 El concepto de ciber criminalidad organizada

Es a partir de la Convención de las Naciones Unidas contras la Delincuencia Organizada Transnacional que se establece que los países parte adopten institutos procesales que permitan la investigació, persecución y consecuente sanción de delitos contra el orden económico y financiero; el comercio y contrabando de estupefacientes, la asociación ilícita, el terrorismo, la trata de personas, la facilitación de la prostitución y la corrupción de menores. Comúnmente son estos delitos los que se asocian con el “crimen organizado”.

Este concepto dentro del que podríamos asimilar el contenido en nuestro derecho interno al hablar del delito de “asociación ilícita”, resulta mejor definido por la referida Convención. El texto internacional estipula, en su art. 2 c), el concepto de “grupo estructurado”, supliendo algunas de las fallas que generalmente se le critican a la figura del art. 210 del Código Penal Argentino. Así el texto indica: “se entenderá un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada”. Con esto se define a los grupos que encabezan las actividades criminales con los números más llamativos en este siglo.

Ahora bien, como se refleja el texto de una Convención de comienzos del siglo XXI en el contexto actual que atravesamos. Es cierto que sus herramientas fueron útiles y, a pesar de algunas críticas, seguirán siéndolo, al menos por un tiempo. Pero necesariamente debe hablarse de un cambio en el contexto en que se aplican estos institutos procesales que con acierto definieron los Estados miembros hace ya veinticuatro años.

Es evidente, que en Argentina los números de criminalidad organizada no parecen ser tan alarmantes como en otros Estados de Latinoamérica, especialmente atendiendo a la ausencia de una extrema violencia que caracteriza a otras regiones. Sin embargo, esto no la deja exenta de la existencia de grupos criminales que operan muchas veces desde el anonimato.

El diario digital "La Prensa" reflejaba en el año 2023, que conforme a la segunda edición del informe del *Organized Crime Index*, creado por la *Global Initiative Against Transnational Organized Crime*, la República Argentina obtuvo un puntaje de 5.00, lo que representa un empeoramiento de 0.63 puntos respecto a 2021 y un aumento de 30 posiciones por su grado de criminalidad organizada, pasando del puesto 125 al 95.[4] Este índice nos permite observar un escalamiento en la cantidad de casos de *ciber* criminalidad. En tal sentido, el mismo medio resume que los delitos financieros habilitados por la *ciber* delincuencia son comunes en Argentina.

Como se ha señalado en el título anterior, el escenario en que se cometen determinados delitos se ha visto ampliamente modificado. En este contexto, la pandemia y el ASPO por COVID-19, solo han favorecido el incremento de *ciber* criminalidad, como se ha visto en los informes estadísticos referidos. Pero ante esta nueva puesta en escena no es posible hablar de casos aislados o de criminales independientes, pues se ha hecho notorio el aumento de casos de grupos criminales que operan a través de medios digitales, dando paso a una era de ciber criminalidad organizada. Y es que aunque parezca una obviedad el concepto de la ciber delincuencia organizada, nutrido por la definición de la Convención, es en simples palabras eso: un grupo formado más allá de un caso fortuito destinado a cometer delitos en el ciberespacio o a través de medios digitales, exista o no funciones predefinidas, tenga o no continuidad de miembros y pese a no tener una estructura organizada.

2.2 La Ley N° 27.319 y algunas de sus deficiencias

La Ley N° 27.319 surgió a raíz del art. 20.1 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, donde se incluía el título de "Técnicas especiales de investigación". En este sentido, el mencionado artículo hace referencia a que siempre que los principios fundamentales del ordenamiento,

[4] Wassi, E.. (2023). "Ciberdelito y crimen organizado en Argentina". La Prensa. https://www.laprensa.com.ar/Ciberdelito-y-crimen-organizado-en-Argentina-535497.note.aspx

las posibilidades y las condiciones del derecho interno de cada Estado miembro lo permitan se deben adoptar las medidas necesarias para permitir la implementación de estas técnicas. Lo curioso es que dentro de esta Convención, se hace mención a la “vigilancia electrónica”, pero sin mayor desarrollo, quedando este concepto, dentro de nuestro país, limitado a las “tobilleras electrónicas”.

A pesar de la demora en la implementación del texto convencional, en el año 2016 se sancionó en la República Argentina la Ley N° 27.319, con la cuál se abrió un nuevo mundo de posibilidades en lo que respecta a la investigación de delitos complejos. Sin embargo, el proceso aún requiere mejoras en algunos puntos. En este sentido, es de destacar que las herramientas contenidas por esta ley especial se limitan a los casos de investigaciones complejas, pero que no comprenden todos los supuestos en los que, en la actualidad, se emplean medios o instrumentos digitales para cometer delitos. Por ejemplo, la ley no aborda todos los casos actuales en los que los medios digitales se utilizan para cometer delitos, como la manipulación de datos en línea o la difusión de material ilícito a través de redes sociales.

2.3 Investigaciones complejas: Su alcance en un contexto actual

Dentro de los llamados “delitos complejos” quedan comprendidas una cantidad de figuras delictivas que, como señala Luis Enrique Velazco (2003), “resultan difícil de circunscribir”. Algunas de las figuras que el autor señala como comprendidas son el tráfico ilegal de estupefacientes, el secuestro extorsivo, el lavado de dinero o capitales, el tráfico de armas, de automotores sustraídos, la falsificación de moneda, la corrupción de funcionarios públicos, entre otros. Sin embargo, hay que recordar que esto surge de las pautas fijadas por la Unión Europea al elaborar el mandamiento de detención y entrega europeo en su lucha contra el terrorismo internacional, es decir hablamos de un marco realmente complejo, pero que en la actualidad no es el único.

Más tarde, en el año 2016, los ejemplos mencionados en el párrafo anterior, se manifestaron en el listado de los delitos enumerados en el art. 2 de la Ley N° 27.319, es decir aquellos casos en los que puede recurrirse a técnicas especiales de investigación para indagar sobre ellos, prevenirlos y combatirlos. Pero pese a la actualidad de la reforma, es necesario preguntarnos si ¿Podemos seguir manteniendo este concepto limitado de “investigaciones complejas”?

Considero que la respuesta es no. En una actualidad donde el contexto digital ha complejizado la investigación, y correspondiente sanción, de delitos “comunes”, es menester rever las definiciones que guían el actuar del Ministerio Público Fiscal y de los auxiliares del Poder Judicial.

Así es que, el concepto de “delitos complejos” debe abarcar a todos aquellos supuestos en que el contexto pueda favorecer la impunidad de las conductas consideradas delictivas. Los inconvenientes a sortear serán determinar qué tipo de circunstancias son las que complejizan la investigación o favorecen de modo alguno a garantizar la evasión de las responsabilidades penales.

Como se ha dicho *ut supra*, la forma en que se cometen delitos comunes se ha modernizado trasladándose en gran medida al entorno digital. En este sentido, la elección de los medios telemáticos se realiza con una doble finalidad. Por un lado, la facilidad de cometer delitos excediendo las fronteras y superando cualquier tipo de distancia. Por otro lado, pese a lo que comúnmente se piensa, no resulta tan sencillo rastrear el origen de las comunicaciones, lo que en algún sentido termina favoreciendo que muchos casos queden impunes.

Es en este contexto, en que las circunstancias relacionadas con los medios elegidos para cometer ciertos delitos termina complejizando la investigación de lo mismo. Esto, a mi entender, fundamenta la necesidad de dictar una reforma legislativa en la materia que posibilite la utilización de las técnicas especiales de investigación previstas en la norma vigente, como así también aquellas que puedan diseñarse especialmente para afrontar estos inconvenientes en la lucha contra la cibercriminalidad.

3. Evidencia digital

En las investigaciones complejas de esta etapa del siglo XXI, la evidencia digital es una de las principales herramientas para lograr la condena por hechos delictivos. Sin embargo, las previsiones legales respecto a este término y otros aspectos relacionados no son del todo precisas.

Como señalé anteriormente (Resoagli, 2023) la evidencia digital debe ser entendida como “todo aquel elemento que, conformando un conjunto de datos, permite esclarecer la verdad de los hechos mediante herramientas electrónicas, sistemas automáticos, dispositivos u otros recursos tecnológicos capaces de procesar y/o almacenar información”. Tomando en cuenta esto, entiendo que el

espectro de la evidencia digital se ve comprendido de una forma apropiada, resultado suficiente para alcanzar diferentes aspectos.

Un punto de gran relevancia, es analizar el cómo llegamos a obtener la evidencia de estas características. En ese camino nos encontraremos con lo que he llamado “el camino hacia la evidencia digital” (Resoagli, 2023), pero más allá de esas consideraciones, merece un especial tratamiento lo referente a las técnicas especiales de investigación. Y en este punto, específicamente las relacionadas con las reformas en torno a la evidencia digital.

En materia de investigaciones por medios telemáticos, el régimen procesal nacional deja mucho que desear, y como ha sido costumbre, fueron algunas provincias las que innovaron en la concreción de figuras y otro tipo de previsiones legales que buscan mejorar el panorama. El caso de algunas reformas legislativas interesantes se encuentra en provincias como Corrientes, pero más recientemente en las leyes adoptadas por el distrito de Mendoza.

4. Comparaciones entre los regímenes vigentes: Técnicas especiales de investigación y evidencia digital

Para esta sección, no se analizarán los pormenores que presenta la Ley de N° 27.319, pues ese ya es objeto de muchos artículos. Lo que se busca es resaltar las mejores reformas legales introducidas al sistema procesal penal de diferentes jurisdicciones de nuestro país, en materia de técnicas especiales de investigación y, en particular, las relacionadas con la evidencia digital.

A fin de contextualizar la situación, es necesario recordar que años antes de la introducción de la figura del agente encubierto, ya se hablaba de la necesidad de legislar su existencia. Esto tomando como punto de partida la Convención de Budapest, pero resaltando la opinión de, por ejemplo, el Tribunal Europeo de Derechos Humanos. Este órgano, resaltó que “el uso de agentes encubiertos debe evitar traspasar los límites de su trabajo de investigación y convertirse en provocador”[5]. Así el primer paso para seguir las directivas internacionales en la materia fue regular apropiadamente las figuras de “agente encubierto” y “agente revelador”, distinguiéndose de la tercera figura, el “agente provocador”, repudiado por doctrina y jurisprudencia como inconstitucional.

[5] Causa Texeira de Castro vs. Portugal, Judgement 9/6/1998-Report of Judgement and Decisions-1998/iv-1464. Tribunal Europeo de Derechos Humanos.

Habiendo hecho esa aclaración, resulta pertinente señalar que en la actualidad existen dos leyes que deberían ser tomadas como pilares para las reformas en materia de evidencia digital en esta nueva generación que ha tomado fuerza desde la sanción de la Ley N°27.319. Estas nuevas regulaciones introducidas a códigos procesales de dos jurisdicciones, corresponden a las provincias de Corrientes (2019) y Mendoza (2024).

4.1 El Código Procesal Penal de la Provincia de Corrientes: Lo mejor del CPPN y del CPPF

En su art. 181 el CPP de Corrientes refiere a la incautación de datos. Para ello toma la redacción del art. 151 del Código Procesal Penal Federal, pero realiza cambios importantes. Como lo he señalado anteriormente (Resoagli, 2023) existen mayores precisiones en la redacción del texto correntino, aunque no por ello la previsión es perfecta.

Sin embargo, considero acertado reconocerle al texto provincial la atención prestada a una cuestión que en el sistema federal parece haberse pasado por alto. Y es que, si bien existe jurisprudencia al respecto, en materia de actos irrepetibles o medidas irreproducibles, todo es muy debatible. Ahora imaginemos un contexto en el que la norma procesal no haga referencia a ellas, la cuestión se vuelve aún más complicada pues atenta contra los derechos de los procesados y en este sentido le quita validez a las respuestas que pretenda brindar el sistema penal. Pues bien, esto es lo que ocurre con el texto del Código Procesal Penal Federal, donde el legislador olvidó mantener la previsión del antiguo código.

En este aspecto, el CPP de Corrientes, prevé expresamente en su art. 160 las medidas de carácter irrepetible indicando:

“El fiscal deberá garantizar el control de las demás partes en la realización de medidas de prueba que, por las características de su producción, podrían resultar irrepetibles, salvo que, existiendo urgencia, las especiales circunstancias del caso no hicieren posible la notificación previa. Los actos serán registrados en soporte audiovisual, si fuere posible.”

La previsión parece acertada, tomando una de las mejores cosas que nos dejó el código de tinte mixto que aún rige la mayoría de los procesos penales a nivel nacional. La actualización de la disposición contenida, por decirlo de algún modo, principalmente en el art. 138 del CPPN, contempla los casos de urgencia

permitiendo adoptar medidas incluso en casos que antes podrían haber sido discutidos.

Si bien es cierto, que la jurisprudencia no es unánime en esta cuestión, hay que considerar que el secuestro de evidencia digital (lo que hoy en día recibe el nombre de incautación de datos) reviste el carácter de una medida o acto irreproducible o irrepetible, según el código al cual se acuda. Ahora bien, la discusión se da en base al desconocimiento sobre el funcionamiento de los medios telemáticos y sobre como asegurar su integridad, pero esto ya lo he planteado anteriormente (Resoagli, 2023). Lo que realmente interesa comprender es si las previsiones actuales permiten realizar esta interpretación de la incautación de datos como una medida que al realizarse reviste características que hacen imposible su reproducción en iguales condiciones. Considero que la respuesta es sí.

Principalmente, el texto correntino es una derivación del modelo federal, pero a diferencia de este, el legislador provincial recordó las previsiones sobre la materia en controversia. Así es que al prever su reforma, se inspiró en el art. 136 del CPPN, cuyo texto reza: “Cuando el funcionario público que intervenga en el proceso deba dar fe de los actos realizados por él o cumplidos en su presencia, labrará un acta en la forma prescripta por las disposiciones de este Capítulo. A tal efecto, el juez y el fiscal serán asistidos por un Secretario, y los funcionarios de policía o fuerzas de seguridad por dos testigos, que en ningún caso podrán pertenecer a la repartición cuando se trate de las actas que acrediten los actos irreproducibles y definitivos, tales como el secuestro, inspecciones oculares, requisa personal.” Considérese especialmente el final del articulado cuando expresa como supuestos de actos irreproducibles y definitivos los relacionados al secuestro, inspecciones oculares o la requisa personal. Al comparar estas actuaciones físicas o corpóreas con las que pueden realizarse sobre un sistema informático o medio de almacenamiento de información, las diferencias no son tan grandes. Como se ha señalado, el secuestro de bienes y el de información, aunque reciba otro nombre, no es tan diferente pues sigue implicando un acto de apoderamiento sobre elementos que pueden ser herramientas o resultado de un delito. En relación a las inspecciones oculares, la explicación es más sencilla, pues la revisión de un ordenador o de la información almacenada en la “nube” implica una mayor vulneración, en la mayoría de casos, de la privacidad de las personas sometidas a estos procedimientos. Esto se debe a que en la actualidad, el común de la sociedad acostumbra a tener respaldos de sus

fotografías, registros de ubicaciones, agendas, sistemas de identificación y de seguridad almacenados en la “nube”. Finalmente, lo que refiere a la requisa personal, merece una explicación similar al anterior ejemplo, pues en el contexto actual del desarrollo de las TICs, resulta igual de, o incluso más, invasivo realizar esta medida que vulnerar la seguridad de un dispositivo de almacenamiento.

Por todo ello, es necesario señalar que la previsión del art. 160 del CPP de Corrientes, en relación con el art. 181 del mismo cuerpo legal, forman una norma necesaria y adecuada para regular la utilización de la evidencia digital en un proceso.

Sin embargo, pese a los aciertos del modelo correntino, hay que resaltar una deficiencia en lo que respecta a la utilización de medidas especiales de investigación. En su art. 213 *in fine* señala: “Las medidas especiales de investigación serán de aplicación sólo en la investigación de delitos de especial gravedad.”

El problema de esta previsión, es que no define adecuadamente los delitos a los que resultaría aplicable, y tampoco remite a los delitos contenidos por la ley nacional. Aunque en este último sentido, podríamos acudir a ella de forma supletoria para cubrir el vacío legal, lo cierto es que la solución no sería del todo adecuada. Por otro lado, el término “delitos de especial gravedad” nos remite al art. 277 inc. 3 a) del Código Penal, cuando refiere a una agravante del encubrimiento usando la misma fórmula. Seguidamente la ley señala que un delito de estas características es “aquel cuya pena mínima fuera superior a tres (3) años de prisión”. Tomando en cuenta esto, podría circunscribirse la aplicación de las medidas especiales de investigación a aquellos delitos con una pena mínima mayor a tres años, pero esto es solo una interpretación en base a la previsión de una figura en particular. Por esto es que esta previsión no es la mejor y requiere una reforma apropiada.

4.2 La Ley N° 9.510 de la Provincia de Mendoza: Técnicas especiales de investigación, evidencia digital y nuevos paradigmas

Esta reforma se sancionó a comienzos del año e implicó una importante modificación al régimen procesal penal en la provincia de Mendoza. Si bien es cierto, que aún no pueden apreciarse del todo los efectos que tendrá esta legislación para el sistema penal provincial, pueden hacerse algunas previsiones y consideraciones al respecto.

a) Técnicas especiales de investigación

En el art. 29 del Código Procesal Penal de la provincia de Mendoza, Ley N°6.730, puede apreciarse una notable evolución en lo que refiere a las disposiciones relacionadas al agente encubierto, y otras figuras relacionadas. Originalmente, se puede apreciar la influencia del sistema mixto, donde el fiscal de instrucción o el Juez de Garantías tenían la facultad de ordenar, por resolución fundada que se procediera a una actuación en cubierta. Posteriormente, mediante la Ley N°9.040, se modificó el articulado y la facultad quedó reservada al Fiscal de Instrucción quien por resolución fundada, gozaba de esta potestad de ordenar el tipo de investigación especial. Actualmente, por imperio de la reforma introducida por medio de la Ley N°9.510, el art. 29 bis, refiere a que la facultad de solicitar la utilización de la actuación encubierta, es exclusiva del Fiscal de Instrucción, pero debe ser requerida ante el "Juez Penal Colegiado"[6]. Con este breve *racconto* de la evolución legislativa en materia de actuaciones encubiertas, se pretende remarcar la influencia que ha tenido el modelo acusatorio y adversarial en el respeto de las funciones que le compete a cada parte en el proceso.

Por otro lado, es necesario señalar que el texto del art. 29 previo a la reforma introducida por la Ley N° 9.510, regulaba de un mejor modo el criterio utilizado para limitar la utilización de este tipo de investigaciones. En este sentido, el texto anterior decía que para las investigaciones por delitos con penas mayores de tres años, podría ordenarse la actuación encubierta. Esta fórmula resuelve el problema interpretativo que podría ocasionar el régimen correntino, y que ha replicado la norma procesal mendocina al delimitar la utilización de las técnicas especiales de investigación en función de si se trata de "delitos de especial gravedad".

Lo novedoso del articulado es la expresa mención que realiza sobre el agente encubierto digital. Cabe realizar la siguiente pregunta: ¿Era necesaria una regulación específica del agente encubierto digital? Aquí, cabe remontarnos a la opinión vertida en el año 2011 por el abogado Hugo Vaninetti, quien reflexionaba sobre lo interesante que resultaría legislar sobre el "ciberpatrullaje"[7]. Y la respuesta por parte de la legislación llegaría por medio de la reforma a la norma ritual de Mendoza.

---

[6] En relación, ver Disposiciones transitorias Ley 9.040. Art. 85 (...) b) Donde dice Juzgado de Garantías, Juzgado Correccional, Juzgado de Ejecución se entenderá Juez Penal Colegiado. c) Donde dice Juez de Cámara se entenderá Juez de Tribunal Penal Colegiado

[7] VANINETTI, Hugo A. (2011) "Agente encubierto y la pornografía infantil en internet" Revista Doctrina Judicial Año XXVIII La Ley. p.9

Es cierto que de la previsión original, tanto de la norma mendocina como de otras semejantes, podría interpretarse la extensión analógica del ámbito en el cual puede actuar el agente encubierto. Sin embargo, contar con una norma que regule específicamente la materia, resultará siempre lo más adecuado. Esto es así porque el hecho de que esté plasmado en una norma imperativa que regula formas y requisitos, otorga seguridad jurídica a todo el proceso penal.

En suma, en el caso particular de la provincia de Mendoza, la regulación específica del agente encubierto digital no solo mejoró la redacción del art. 29, al agregar la previsión del art. 29 bis, que se convirtió en un mejor reflejo de los principios del modelo acusatorio y adversarial. Por lo que, tomando en cuenta ambos beneficio y retomando la pregunta original: sí, resultaba necesaria la regulación específica del agente encubierto digital.

b) Evidencia digital

Conferencistas estadounidenses, como Martín Sabelli, han señalado la importancia de contar con un "Código de Evidencias", el cual puede ser entendido como aquella norma que reúne los principios y disposiciones que permitan el correcto tratamiento de las evidencias y el camino a seguir hacia, y hasta, su conversión en prueba. Y si bien, el Código de Evidencias debe ser una aspiración procesal en lo que respecta a todos los medios de prueba, es importante señalar cuando existen avances en al menos algún tipo de ellas.

Considero que, comparando dos legislaciones tan modernas como lo son el Código Procesal Penal de Corrientes y la Ley N°9.510 de Mendoza, existen notables diferencias en lo que refiere al tratamiento de la evidencia digital. Pese a su gran intento por introducir al sistema procesal correntino a una nueva fase de modernización, no se ha logrado alcanzar el 100% de la misma. Y esto se evidencia particularmente al denotar la falta de precisiones en cuanto al tratamiento de cuestiones como la incautación de datos y los procedimientos relacionados.

En este caso, la Ley N°9.510 expresa pautas más claras al respecto. Con la introducción del art. 228 bis al Código Procesal Penal de Mendoza, se fijan normas y requisitos sobre el secuestro, apertura y análisis de sistemas informáticos y los que son propios de la incautación de datos. Así en el tercer párrafo, menciona que recae en cabeza del Fiscal el deber de indicar al juez: "a) La individualización de los dispositivos o sistemas informáticos que serán objeto del registro, b) Una descripción del objeto concreto de la medida, c) La identificación de los

mecanismos, metodología y herramientas mediante los cuales se almacenará la información obtenida que permitan asegurar la integridad de los datos y el resguardo de la cadena de custodia, d) El funcionario y/o quien designe como encargada de la ejecución del registro, copia o incautación de datos.”

Con estas breves cuatro líneas, la provincia de Mendoza ha dado un inmenso paso en lo que respecta a legislar sobre reglas de evidencia. Estas previsiones innovadoras marcan el rumbo a seguir, y permiten delimitar las facultades de la acusación a la hora de investigar a través de medios digitales, otorgan seguridad jurídica a los imputados, actuales y eventuales, y, sobre todo, garantizan la plena vigencia de un estado de derecho sostenido en un sistema procesal penal acusatorio y adversarial.

Conclusión

En conclusión, el análisis detallado de las técnicas especiales de investigación y su relación con la evidencia digital dentro del marco de la legislación vigente, situando la cuestión en dos regímenes muy modernos, como lo son el de Corrientes y el de Mendoza, revela una necesidad inminente de actualización y adaptación pese al trabajo realizado hasta el momento. Ya no es factible que las autoridades se conformen con las previsiones contenidas por la Ley N° 27.319.

El crecimiento exponencial de los delitos cibernéticos y la evolución de las formas de cometerlos han superado los límites que la legislación actualmente establece, evidenciando la urgencia de revisar y modificar los marcos normativos existentes. La admisión y tratamiento de la evidencia digital en los procesos judiciales se erige como un desafío clave, requiriendo criterios claros y actualizados para su validez y uso. En este sentido, es menester poder ampliar los casos en que puede requerirse a técnicas especiales de investigación y aprender a definir de un modo adecuado los límites y requisitos que se le otorgan a la acusación a la hora de solicitarlas y ejecutarlas.

Solo mediante un enfoque proactivo y colaborativo entre legisladores, expertos en tecnología y profesionales del derecho se podrá garantizar una regulación efectiva y justa que responda a los desafíos de la era digital. Considero que este es el camino que debe seguirse para que, a futuro, podamos contar con normas claras que terminen de perfeccionar nuestro sistema procesal penal.

Bibliografía

ABOSO, Gustavo E. (2022) “Fraudes, Sabotaje y extorsión online en la moderna sociedad de la tecnología”. Editorial ElDial.com. p. 11-21.

AROMÍ, María Gabriela A. (2022) “Manual de Derecho Procesal Penal: Visión constitucional” Editorial ConTexto.

DIRECCIÓN OPERATIVA DEL COMITÉ EJECUTIVO PARA LA LUCHA CONTRA LA TRATA DE PERSONAS (2019) “Grooming y trata” https://www.argentina.gob.ar/sites/default/files/2019/12/grooming_y_trata.pdf

RESOAGLI, Juan M. (2023) “De la evidencia a la prueba digital: Problemáticas aparejadas a la producción en el proceso penal de la provincia de Corrientes”. Libro: “Proceso Penal: Gestión del conflicto en el sistema acusatorio”. Editorial ConTexto. p.189-198.

ROIBÓN, María Milagros (2024) “El agente revelador en la legislación argentina”.https://www.pensamientopenal.com.ar/doctrina/91162-agente-revelador-legislacion-argentina

UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA (2021). “Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020”. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). https://www.fiscales.gob.ar/wp-content/uploads/2023/12/UFECI_informe-de-Gestion_23_15-12.pdf

UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA (2023). “Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022-2023”. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). https://www.fiscales.gob.ar/wp-content/uploads/2023/12/UFECI_informe-de-Gestion_23_15-12.pdf

VANINETTI, Hugo A. (2011) “Agente encubierto y la pornografía infantil en internet”. Revista Doctrina Judicial Año XXVIII La Ley. p.1-9.