REVISTA TEKOANDU
Revista Universitaria de Filosofía y Educación
ISSN/ISSN-L: 3006-2667

TÉCNICAS ESPECIALES DE INVESTIGACIÓN
SPECIAL RESEARCH TECHNIQUES

Juan Pablo Mendoza Benítez
jpmendozabenitez@gmail.com
Universidad Jesuita del Paraguay

RESUMEN

Las técnicas especiales de investigación son recursos incorporados a partir de Convenciones internacionales con miras a afrontar el desafío que suponen las organizaciones criminales trasnacionales, poniendo en manos de los investigadores recursos que permiten investigar en tiempo real a estas organizaciones. Los operadores del sistema deben, a este respecto, conocer adecuadamente las características y alcances de cada una de estas técnicas, así como el grado de injerencia que estas técnicas suponen dentro del ámbito de los derechos y garantías constitucionales, a los efectos de su adecuado control. A estas técnicas se le han sumado en los últimos años, medios de investigación tecnológicos, que incorporados a la Convención de Budapest sobre Cibercrimen, permiten a los países signatarios de la Convención emplear modernos recursos de investigación, para el entorno informático. Sin embargo y no obstante, dichos recursos de investigación deben ser objeto de una adecuada regulación por parte de cada país signatario, a fin de permitir a las fuerzas públicas emplear de forma legal estas técnicas, que resultan ser indispensables en el panorama actual.

Palabras clave: Cibercrimen, injerencia, técnicas especiales, organizaciones criminales.

ABSTRACT

Special investigative techniques are resources incorporated through international conventions to address the challenge posed by transnational criminal organizations, providing investigators with resources that allow for real-time investigations of these organizations. In this regard, system operators must adequately understand the characteristics and scope of each of these techniques, as well as the degree of interference they pose within the scope of constitutional rights and guarantees, for the purposes of

ISSN/ISSN-L: 3006-2667

their adequate control. In recent years, technological investigative means have been added to these techniques. Incorporated into the Budapest Convention on Cybercrime, these techniques allow signatory countries to employ modern investigative resources for the cyber environment. However, these investigative resources must be adequately regulated by each signatory country to allow law enforcement to legally employ these techniques, which are essential in the current environment.

Keywords: Cybercrime, interference, special techniques, criminal organizations.

RESULTADOS

La aparición de las organizaciones criminales con gran volumen de recursos económicos, y de alcance trasnacional, supuso un desafío bastante relevante para los operadores de la ley de cada país, limitados por las exigencias propias de la jurisdicción y la soberanía de sus respectivos Estados, limitación que siempre ha supuesto una ventaja apreciable a favor de las actividades delictivas.[1]

Pero además del obstáculo supuesto por la jurisdicción limitada por las fronteras de los propios Estados, estas organizaciones criminales presentan características y circunstancias que dificultan la investigación de sus actividades. A este respecto podemos mencionar la tradicional estructura jerárquica de corte piramidal, donde existe un jefe máximo, en otro nivel sus capitanes (como gerentes operativos), y a otro nivel inferior los soldados (operarios que realizan las tareas "sucias" de la organización); además, quienes acceden a integrar estos grupos delictivos pasan frecuentemente por verdaderos rituales de iniciación que buscan comprometer al máximo la lealtad del nuevo integrante, con juramentos de silencio y compromiso. Este nivel de jerarquización, y fidelización (cuya infracción es pagada frecuentemente con la propia vida), ha sido tradicionalmente otro factor que dificulta la investigación de las actividades delictivas de la organización

[1] Siempre han existido organizaciones criminales, como las Triadas de China; la Yakuza japonesa; o los Assasins de medio oriente. Sin embargo, en el presente trabajo hacemos referencia a una configuración actual de tal concepto, caracterizado por su alcance trasnacional; su manejo de enormes recursos financieros; sus influencias en la economía y la política; el empleo de la violencia en un contexto de impunidad creado por sus recursos, y su creciente riesgo para la existencia de la democracia.

ISSN/ISSN-L: 3006-2667

mediante las técnicas tradicionales de investigación[2]. En respuesta a estos desafíos, presentes específicamente en la investigación de los delitos cometidos por organizaciones criminales con un despliegue muchas veces trasnacional, se implementaron medidas de investigación necesarias y efectivas con el fin de hacer posible la sanción de los responsables de estos hechos.[3]

Los operadores de la justicia, vieron la necesidad de infiltrar a las organizaciones criminales a los efectos de establecer su estructura interna, su jerarquía, sus integrantes, y su forma de operar, para lo cual se recurrió reclutar agentes policiales, capacitarlos e introducirlos a la organización criminal investigada, única vía, en muchos casos, para obtener información fidedigna sobre la organización, a partir de lo cual surge la figura del "agente encubierto". Como mecanismo para establecer la manera en la que estas organizaciones operaban, se organizaron operaciones encubiertas, en donde se permitía a la organización criminal, realizar sus actividades delictivas ordinarias, bajo vigilancia y control de las autoridades, a fin de identificar a los participantes, la forma de operar, las vías empleadas y métodos, lo que define a la técnica de las operaciones encubiertas, y también a las entregas vigiladas, otras modalidades de técnicas especiales.

Para poder establecer el tipo de participación de un sospechoso en el contexto de una organización criminal, resultaba indispensable el poder contemplar sus actividades por marcos extensos de tiempo, para lo cual se estableció la observación, vigilancia y seguimiento de los sospechosos por parte de equipos de agentes de policía, lo que permitía revelar las conexiones del sospechoso con la organización, sus contactos, así como sus actividades. De esta forma se fueron perfilando tres de las principales técnicas de investigación especiales, dispuestas para la lucha contra las organizaciones criminales: agentes encubiertos, entregas vigiladas, además de la observación, vigilancia y seguimiento. Estas tres primeras técnicas de investigación fueron incluidas en acuerdos internacionales muy relevantes para el combate del crimen organizado trasnacional, en

[2] Con dicha denominación hacemos referencia aquellas técnicas que como el interrogatorio a testigos, el pedido de informes, la realización de estudios periciales, se realizan con posterioridad a la noticia de la comisión de un delito, y que además apuntan a descubrir la existencia de esos hechos pasados, al igual que a sus partícipes.

[3] Por supuesto, esto fue el resultado de un largo proceso de "prueba y error", por parte de las fuerzas policiales en su afán por castigar los delitos atribuidos a estas organizaciones criminales, en un desarrollo histórico que abarca desde el primer cuarto del siglo pasado, con las actividades de la mafia de Chicago, en épocas de la prohibición del alcohol; o el surgimiento de las cinco familias del crimen en Nueva York.

ISSN/ISSN-L: 3006-2667

primer término a la Convención de las Naciones Unidas sobre Sustancias Estupefacientes y Psicotrópicas, de Viena de 1988 (Ley 16/90). Posteriormente, se sumó la Convención de las Naciones Unidas sobre Delincuencia Organizada Trasnacional, de Palermo, del año 2000 (Ley 2298/2003). Por su parte, en el año 2003, aparece la Convención de las Naciones Unidas contra la Corrupción, firmada en Mérida (México) (Ley 2545/2005). Estas convenciones han sido ratificadas por la República del Paraguay, convirtiéndose en parte del ordenamiento legal de la nación.

Con posterioridad, han sido incorporadas al catálogo de técnicas especiales otras modalidades y recursos de investigación. Se las denomina técnicas especiales de investigación por oposición a las técnicas ordinarias empleadas comúnmente en la investigación penal. En la investigación de un delito, normalmente el investigador inicia sus pesquisas con posterioridad al conocimiento de un hecho que reúne las características de ser un delito, a priori, acontecido en tiempo pasado, para lo cual requiere la declaración de testigos, directos o de referencia; solicita informes periciales; recauda evidencias e indicios sobre lo sucedido; orientando su labor investigativa a la reconstrucción de un hecho acontecido en el pasado, en base a un razonamiento abductivo.

Por el contrario, en la investigación de delitos atribuidos a organizaciones criminales, las técnicas especiales permiten al investigador realizar pesquisas en etapas previas incluso al inicio de la ejecución de los delitos, y durante la realización de los actos ejecutivos del delito, lo que otorga a la investigación mayor dinamismo desde que la misma se efectúa de manera simultánea a la realización del hecho punible, por tanto, sus herramientas no apuntan a una realización del pasado, sino a una ejecución presente o futura.

Las características antes señaladas obligan a que el empleo de este tipo de técnicas deba ser rigurosamente legislado y acotadas, ya que por un principio de proporcionalidad, las mismas deben emplearse tan sólo en la investigación de hechos de especial gravedad, como son las realizaciones delictivas de las organizaciones criminales.

Entre los objetivos del empleo de este tipo de técnicas se encuentra: La identificación precisa de una organización criminal; la descripción de sus actividades; la determinación de sus integrantes y sus estructuras jerárquicas; el descubrimiento de sus fuentes de financiamiento; la recolección de la prueba para acreditar en juicio los aspectos anteriores.

Reiteramos que no resulta posible, por un principio básico de proporcionalidad, el empleo de este tipo de técnicas en la investigación de cualquier tipo de hecho punible, sino sólo

ISSN/ISSN-L: 3006-2667

en los delitos que tengan que ver con organizaciones criminales. Esto se explica en el grado de injerencia que el empleo de estas técnicas especiales de investigación supone en la esfera de los derechos y garantías constitucionales de los sospechosos y de las personas vinculadas a la investigación.

En el catálogo de las técnicas especiales de investigación legisladas en el derecho positivo paraguayo podemos encontrar:

1. Operaciones encubiertas: Consisten en la puesta en marcha de operaciones engañosas que apuntan a simular la realización de actividades delictivas, mediante engaños y artimañas, preservando la confidencialidad sobre la identidad de las personas que participan activamente en ellas, empleando agentes encubiertos, con la finalidad de incautar mercaderías prohibidas, drogas o activos pertenecientes a organizaciones criminales; así como recabar pruebas para el enjuiciamiento de sus responsables.
2. Entrega vigilada: Esta técnica permite el transporte y tránsito ilícito de sustancias estupefacientes, con conocimiento y bajo vigilancia de las autoridades, a los efectos de establecer las vías de tránsito, formas de entrada y salida del país, el sistema de distribución y comercialización de estas sustancias.[4]

La entrega vigilada permite, con la autorización jurisdiccional correspondiente, la perpetración de un hecho consistente en un delito de entrega de sustancias estupefacientes prohibidas, pero bajo el control de las autoridades, de tal suerte que los perpetradores puedan ser aprehendidos al tiempo mismo de la entrega de la mercadería prohibida, o tiempo después. Entre las ventajas de este tipo de procedimiento se encuentran el hallar al descubierto a los perpetradores al tiempo de la entrega de la sustancia prohibida, constituyendo con ello una prueba innegable de su participación en el hecho ilícito; a esto se debe agregar que esta técnica permite establecer las rutas y técnicas operativas comúnmente utilizadas por las organizaciones criminales para sus entregas; finalmente,

[44] Art. 84, ley 1340/88: "Se entenderá por procedimiento de entrega vigilada la técnica de investigación que permite que el transporte y tránsito ilícito o sospechoso de estupefacientes o demás drogas peligrosas, conocido y vigilado por las autoridades, no sea momentáneamente impedido, a fin de descubrir las vías de tránsito, el modo de entrada y salida del país, el sistema de distribución y comercialización, la obtención de elementos probatorios o la identificación de los organizadores, transportadores, compradores, protectores y demás participes del tráfico ilegal, sea en el país o en el extranjero y la incautación de la droga así como la detención y procesamiento de los organizadores, transportadores, compradores, protectores y demás partícipes, y posibilitar que la autoridad proceda lícitamente de acuerdo con las pautas establecidas en este capítulo."

ISSN/ISSN-L: 3006-2667

el empleo de esta técnica permite identificar a los funcionarios corruptos que colaboran con las organizaciones criminales. La entrega vigilada requiere de una gran coordinación entre los operativos encargados de ejecutarla, debido a que cualquier apresuramiento con la intervención tendrá por consecuencia la frustración de la operación, impidiendo obtener los resultados deseados. Cuando la entrega vigilada se realiza dentro del territorio de un solo estado, la responsabilidad total del operativo depende de las autoridades nacionales del estado del que se trate, sin embargo, es común que este tipo de operativos se realice afectando el territorio de dos o más estados, por lo que en ese tipo de casos se requiere de una gran coordinación entre las autoridades de cada uno de los estados afectados.

3. Agente encubierto: es, conforme a la legislación paraguaya, un agente especial que voluntariamente acepte participar en operaciones encubiertas o en entregas vigiladas autorizadas judicialmente, con la obligación de actuar de forma secreta o bajo identidad falsa.[5]

Este tipo de técnica implica un alto riesgo para la integridad y la vida de los agentes que se encargan de llevarla adelante, ya que supone que el agente, bajo identidad falsa y mediante engaños o artimañas, se infiltre y formen parte de una determinada organización criminal durante un tiempo que puede ser prolongado. No olvidemos que el absoluto secreto sobre la identidad del agente encubierto es una condición esencial para el éxito de la medida de investigación, y por lo mismo, sólo debe existir un enlace que contacte al agente, para la presentación de sus informes, con el Fiscal a cargo de la investigación, a los efectos de evitar las filtraciones y la identificación del agente encubierto por parte de los sospechosos.

El agente encubierto, no puede ser un sujeto improvisado, una persona sin ningún tipo de capacitación, e inclusive tampoco puede ser escogido de cualquier cuadro policial. El aspirante a agente encubierto debe necesariamente salir de las filas de los agentes especiales, personal ya entrenado en las habilidades y recursos de la policía, sin embargo

[5] Art. 96, ley 1340/88: "Son agentes encubiertos los agentes especiales que sean designados por la Secretaría Nacional Antidroga (SENAD) o por el fiscal y que acepten voluntariamente participar en operaciones encubiertas o en entregas vigiladas específicas autorizadas judicialmente, con conocimiento y consentimiento escrito del juez autorizante de cada operativo, y que para el cumplimiento de su cometido actúen de modo secreto o bajo identidad falsa. Terminado su cometido los agentes encubiertos reasumirán de pleno derecho sy condición y función de agentes especiales…"; ver además art. 23 de la ley 4788/12, Integral Contra la Trata de Personas". Confrontar con el art. 27 de la ley 4788/12, Integral Contra la Trata de Personas.

ISSN/ISSN-L: 3006-2667

y no obstante esto no resulta suficiente para que la labor del agente encubierto tenga éxito. Los agentes encubiertos deben, además de la preparación básica del currículo policial, comprender los aspectos culturales característicos del grupo social al que pertenecen los integrantes de la organización en la que se debe infiltrar, como la jerga, los usos y modismos, los saludos, las narrativas propias del grupo, simbolismos y tatuajes. El conocimiento de estos aspectos resulta esencial para que el agente pueda infiltrarse eficazmente dentro de la organización investigada, además de evitar con ello ser descubierto. Resulta esencial que el agente encubierto conozca las particularidades culturales del grupo que debe infiltrar, así como su lenguaje, y sea capaz de reproducir las conductas que se consideran socialmente aptas en el contexto del grupo. Esto nos lleva a otra condición esencial respecto al agente encubierto, consistente en que el mismo debe operar incluso fuera de la ley. La regulación legal del agente encubierto debe permitir que el mismo, bajo ciertas condiciones y límites, pueda realizar hechos antijurídicos, a los efectos de que logres u objetivo de infiltrarse en la organización sin ser detectado. No sería efectiva su participación en caso de que al agente encubierto le estuviese prohibida la comisión de hechos antijurídicos, con lo cual quedaría en evidencia ante los criminales. También resulta esencial que el agente encubierto cuente con el apoyo permanente de un equipo técnico con el poder de decisión sobre la continuidad o no del agente encubierto en la investigación. Este equipo, encabezado por el fiscal asignado a la causa, debe manejar eficientemente los datos a los efectos de determinar si el agente se encuentra atravesando o no una situación de peligro, y retirarlo inmediatamente a los efectos de salvaguardar su integridad y su vida.

La ley permite que el agente encubierto pueda participar en la realización de hechos antijurídicos a los efectos de otorgar credibilidad a su cobertura de encubierto. Por lo común los grupos criminales no otorgan confianza a sus elementos hasta que éstos hayan superado una suerte de bautismo, consistente en la realización de un delito, o la estadía en prisión, sin delatar a sus compañeros del crimen.

4. Observación, seguimiento y vigilancia: es la técnica de investigación consistente en el seguimiento, observación y la fotografía o filmación de los sospechosos y sus movimientos.[6]

[6] Art. 88, ley 1340/88: “El juez podrá autorizar en cada caso y por tiempo determinado, a solicitud de la Secretaría Nacional Antidroga (SENAD) o del fiscal, a que ellos o sus agentes debidamente

ISSN/ISSN-L: 3006-2667

En ocasiones conviene establecer un seguimiento sobre un sospechoso o sobre una operación comercial sospechada de ser la portada de una organización criminal. Para el efecto, se destina a un grupo de agentes con la misión de realizar el seguimiento y observación de un sospechoso, los lugares por donde transita, los contactos que mantiene y las rutinas que realiza. Por lo común el grupo de seguimiento asignado va turnándose cada tanto a los efectos de evitar ser identificados y que con ello que la operación quede en evidencia.

Al seguimiento y la observación de los sospechosos puede además sumarse la toma de fotografías tanto del sospechoso como de las personas con las que el mismo entra en contacto, al igual que los lugares que visita. Sin embargo, el seguimiento y observación de los sospechosos adquiere otro cariz cuando se le suma la filmación. Esto es así debido a que las posibilidades técnicas de los dispositivos de filmación brindan una calidad inusitada al producto final consistente en la grabación de los hechos realizados por los sospechosos. No sólo es factible la filmación en calidad de alta fidelidad, sino además es posible contar con la grabación en audio de las conversaciones del sospechoso, lo cual es factible justamente gracias a los avances de la tecnología.

A este respecto corresponde señalar que existen cámaras basadas en la tecnología del infrarrojo, que posibilitan atravesar las paredes de cualquier construcción ordinaria y captar los movimientos realizados por las personas que se encuentran dentro. Sin embargo y no obstante, el empleo de este tipo de tecnologías requiere siempre de autorización jurisdiccional específica, debido al alto nivel de injerencia que supone sobre las garantías constitucionales del sospechoso, en lo que respecta a la intimidad o la privacidad de la persona sospechosa, como consecuencia de que se trata de imágenes térmicas captadas dentro del recinto privado del sospechoso.

Por otro lado, conviene tener en cuenta que el seguimiento del sospechoso por parte de equipos de agentes es hoy día frecuentemente sustituido por el empleo de dispositivos electrónicos con tecnología GPS (sistema de posicionamiento global). Estos dispositivos pueden presentarse en tamaños muy pequeños y ser adheridos al vehículo del sospechoso, o por su propia vestimenta a los efectos de tener datos ciertos, en tiempo real, y durante las veinticuatro horas de cada día, de cada semana, de cada mes, sobre la ubicación del

individualizados, fotografíen o filmen a los sospechosos y sus movimientos o que intercepten, registren, graben o reproduzcan sus comunicaciones orales, cablegráficas o electrónicas…”

ISSN/ISSN-L: 3006-2667

sospechoso. De esta forma, no se corre riesgo alguno de que el seguimiento pueda ser detectado por el sospechoso, o que el personal encargado del seguimiento se extravíe, o se queden dormidos, o tengan que retirarse de la operación como consecuencia de una urgencia no prevista de carácter humano. A esta ventaja se suma otra de carácter adicional, consistente en que la tecnología GPS resulta ser absolutamente normal y ubicua hoy día en el uso común de las personas, esto es así debido a que normalmente nos rodean distintos tipos de dispositivos que poseen el sistema de ubicación por GPS, como teléfonos o relojes inteligentes. En el caso de los teléfonos inteligentes, es más corriente el contar con este tipo de servicio GPS, ya sea entre las propias posibilidades o servicios insertos en el sistema del teléfono, o en las aplicaciones de telefonía móvil que son masivamente utilizadas por los usuarios de este tipo de servicios. En estas condiciones, los investigadores no tienen la necesidad de "insertar" ningún tipo de transmisor en el vehículo o ropas del sospechoso, sino tan sólo habilitar el sistema GPS del teléfono del mismo y conectarse al mismo a los efectos de poder realizar un seguimiento sin límite temporal alguno sobre el sospechoso[7].

5. Intervención de comunicaciones: otorga al Juez la facultad de disponer la intervención de las comunicaciones del imputado, indistintamente del medio técnico utilizado para conocerlas[8].

Es de señalar que la redacción de la disposición de la ley procesal penal paraguaya que admite esta técnica, art. 200 del Código Procesal penal, resulta clara al señalar la posibilidad de intervenir las comunicaciones del imputado, sin realizar discriminación alguna respecto al tipo de comunicación. En otras palabras, no se hace distinción alguna en relación a si el tipo de comunicación a ser intervenida se refería a las telefónicas; las

[7] A este respecto resulta ilustrativo el voto de la mayoría en el precedente "United States v. Jones" (565 U.S. 400 (2012), respecto al empleo de dispositivos GPS para el seguimiento de sospechosos. En el fallo se señala que "…cuando la combinación de datos provenientes de fuentes que en principio no están constitucionalmente protegidas conforma un "mosaico" que revela mucha más información que cada uno de esos datos considerados individualmente se encuentra en juego el derecho a la privacidad" (Citado por Blanco, Hernán, Tecnología Informática e Investigación Criminal, 1ra.ed., Ciudad Autónoma de Buenos Aires, la Ley, 2020, p 180)

[8] Art. 200, Código Procesal Penal de la República del Paraguay: "El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas. El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior, podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. La intervención de comunicaciones será excepcional"

ISSN/ISSN-L: 3006-2667

realizadas por chat de WhatsApp u aplicaciones análogas; llamadas vía aplicaciones tipo Sky; video conferencias como las empleadas por aplicaciones del tipo Zoom, etc. Incluso, sería factible argumentar que la disposición en análisis admite la intervención de las comunicaciones establecidas por vía de correo electrónico.

Esta disposición admite cualquier medio técnico utilizado para el conocimiento de las comunicaciones cuya intervención fuera dispuesta por el Juez. La habilitación legal señalada permite por tanto echar mano a las modernas tecnologías de investigación en materia informática, en concreto el empleo de los software espías (spyware), elaborados específicamente para introducirse de manera subrepticia en los dispositivos empleados por los sospechosos, a los efectos de extraer información relevante para la investigación. Estos medios técnicos, llamados también troyanos, son programados para la búsqueda de determinadas palabras o secuencia de palabras en los dispositivos de almacenamiento infectados, a los efectos de que una vez detectada la información buscada, el software espía se encargue de enviar al investigador la referida información, sin que el dueño del dispositivo tenga sospecha alguna de lo que está aconteciendo.

La medida requiere de autorización jurisdiccional fundada, bajo pena de nulidad, y tiene carácter excepcional.

6. Intercepción y secuestro de correspondencia: bajo esta medida el juez está facultado a disponer la intercepción o el secuestro (de manera indistinta), de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida al imputado o destinada a él, aunque sea bajo nombre supuesto.[9]

La doctrina suele asimilar a la comunicación epistolar la comunicación a través de correo electrónico, motivo por el cual en la opinión de algunos autores, esta disposición podría servir de base para la intercepción de las comunicaciones realizadas por la vía de correo electrónico. Para tal efecto son de empleo necesario el secuestro del dispositivo del sospechoso con acceso al correo electrónico del mismo, a menos que se haya dispuesto una medida que la doctrina denomina "allanamiento informático", mediante el cual se inocula un troyano o virus espía, sin el conocimiento del sospechoso, en su dispositivo y

[9] Art. 198, Código Procesal Penal de la República del Paraguay: "Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto. Regirán las limitaciones del secuestro de documentos u objetos".

ISSN/ISSN-L: 3006-2667

se procede a extraer la información del correo electrónico, todo con autorización jurisdiccional.

Estas técnicas de investigación han sido incorporadas por diversas vías a la legislación paraguaya, en concreto, en primer lugar fueron incorporadas por vía de las siguientes leyes:

1. Ley 1340/88, Que modifica y actualiza la Ley Nro. 357/72, que reprime el tráfico ilícito de estupefacientes y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes. Ver artículos 82, 84, 86, 96 y concordantes;
2. Ley 4788/12, Integral contra la trata de personas. Ver artículos 23 al 29;
3. Ley 6431/19, Que crea el procedimiento para la aplicación del comiso, el comiso especial, la privación de beneficios y ganancias y el comiso autónomo. Ver artículo 8, actividad probatoria.

La autorización para el empleo de estas técnicas estará siempre en poder de un juez penal, a quien el fiscal asignado a una causa deberá solicitar la autorización respectiva para el empleo de una o varias técnicas especiales de forma simultánea. El fiscal a cargo es quien controla la ejecución de la investigación mediante el empleo de estas técnicas, y quien tiene el poder de decisión sobre el final en la utilización de estos recursos en una investigación, sin embargo, siempre deberá tomar sus determinaciones asesorado por un oficial de las fuerzas públicas, que tendrá a su cargo la planificación estratégica del operativo.

Principios a los que debe ajustarse la realización de las técnicas especiales de investigación:

En este sentido, Guanes Nicoli [10], a quien seguiremos en este capítulo, comenta que existe consenso con relación a los presupuestos que deben orientar una técnica de investigación como la intervención de comunicaciones, a partir de lo cual es posible proyectar los mismos principios sobre el resto de las técnicas de investigación especiales.

[101010] Guanes Nicoli, Manuel, "El Control Jurisdiccional de la Intervención de las Comunicaciones Telefónicas. Especial Referencia a la Legislación Paraguaya", en ILÍCITOS ECONÓMICOS Y EVIDENCIA DIGITAL, Gallo Tagle, Marcelo (et al.); coordinación general de Marcelo A. Peluzzi; Marìa Amelia Expucci; María Alejandra Mendez, 1ra. Edic., Ciudad Autónoma de Buenos Aires; 1ra. Edción, 2022. Pág. 146-149

ISSN/ISSN-L: 3006-2667

a. Proporcionalidad

En este sentido el principio más relevante, a partir del cual adquieren sentido todos los demás principios es el de proporcionalidad. Se trata de un verdadero "principio rector" a la hora de limitar la injerencia en las garantías constitucionales por parte de la persecución penal estatal, ya que establece que los intereses que se buscan proteger mediante la injerencia siempre deben ser más relevantes que los derechos y garantías afectados. A partir de lo cual, mediante este instrumento es posible mensurar los intereses y derechos que entran en juego.

b. Especialidad

Este presupuesto exige que la medida de investigación adoptada esté relacionada con el hecho investigado específicamente. El principio de especialidad requiere que la técnica de investigación a ser adoptada esté relacionada con la finalidad de la investigación. Debido a esta circunstancia, en la resolución que se autorice la realización de esta técnica deberá especificarse el objetivo a ser logrado de forma específica.

c. Idoneidad

Respecto a este principio, la medida de investigación adoptada deberá ser el medio más adecuado para lograr los fines perseguidos, de tal manera que en la perspectiva de un análisis previo, al tiempo de la adopción de la resolución de autorización judicial, surgiere de manera clara la existencia de otras vías idóneas para lograr el fin, deberán ser estas últimas las adoptadas, en procura de una investigación más eficiente.

d. Necesidad o subsidiariedad

De la ponderación de los bienes en juego, que debe ser realizada en la resolución judicial que vaya a autorizar la medida de investigación de que se trate, debe surgir el carácter necesario, o en otras palabras, que la técnica a ser adoptada en cuestión resulte ser el único medio viable para obtener los fines requeridos en el contexto de la investigación.

e. Límite temporal

Una condición esencial derivada del principio de proporcionalidad consiste en la limitación temporal para la realización de la técnica investigativa de que se trate. Los marcos temporales de autorización para la ejecución de cada técnica de investigación deben ser apropiadamente acotados en la resolución judicial, a los efectos de evitar que las injerencias en los derechos y garantías afectados se tornen arbitrarias.

ISSN/ISSN-L: 3006-2667

Nuevas medidas tecnológicas de investigación

Nos merece una mención especial la incorporación en el último lustro de un conjunto de técnicas de investigación aportadas por las tecnologías de la información y la comunicación, principalmente a través de la adopción de la Convención de Budapest sobre Cibercrimen[11], de 2001. Esta Convención es hasta la fecha el único instrumento internacional de combate a la delincuencia en el ámbito informático, de alcance internacional, originalmente elaborada para el ámbito de los países integrantes del Consejo de Europa, con posterioridad otros Estados ajenos a esa órbita fueron adhiriéndose a la Convención.

La Convención de Budapest tiene tres partes principales, la primera en la que se introducen figuras del derecho penal sustantivo (arts. 2 al 13); la segunda, donde se tratan los denominados poderes procesales de investigación (arts. 11 al 22); y una tercera destinada a los mecanismos de cooperación internacional, incluida la red de atención 24/7 (arts. 23 al 35).

El camino de la adhesión de Paraguay a la Convención de Budapest tuvo al menos dos etapas, durante la primera, si bien no se procedió a la ratificación de la convención, sí se incorporaron a la legislación penal sustantiva las figuras típicas descriptas en la Convención. Esto aconteció en el año 2011, con la Ley 4439, que introdujo varias figuras típicas al Código Penal Paraguayo, específicamente se incluyeron: pornografía relativa a niños y adolescentes (art. 140 del Código Penal); acceso indebido a datos (art. 146b del Código Penal); acceso indebido a sistemas informáticos (art. 174b del Código Penal); sabotaje a sistemas informáticos (art. 175 del Código Penal); y estafa mediante sistemas informáticos (art. 188 del Código Penal)

Posteriormente, en el mes de diciembre del año 2017, se produjo la ratificación de la Convención de Budapest por el Congreso paraguayo, mediante la ley 5994. Las figuras del derecho penal sustantivo descriptas en la Convención ya fueron incorporadas con anterioridad al derecho positivo paraguayo, por la mencionada Ley 4439/11, sin embargo, y no obstante, los denominados “poderes procesales de investigación” descriptos en la segunda parte de la Convención, no han sido objeto de regulación. Estos “poderes

[11] En adelante CBC, por sus siglas.

ISSN/ISSN-L: 3006-2667

procesales de investigación" constituyen técnicas que se valen de los adelantos tecnológicos en materia de informática, por lo que su incorporación resulta absolutamente necesaria para otorgar más recursos a los investigadores, pero a la vez requieren de una regulación adecuada por parte del legislativo, a los efectos de resguardar adecuadamente los derechos y garantías consagrados en la Constitución Nacional.

Particularmente, las técnicas de investigación descriptas en la Convención de Budapest son:

1. Conservación rápida de datos informáticos almacenados (art. 16 CBC): otorga la facultad de ordenar a una persona que tenga en su poder datos electrónicos específicos almacenados en algún tipo de dispositivo de almacenamiento de datos, que los conserve de forma rápida. Esta orden se proyecta sobre los denominados datos de tráfico e incluye el deber (por parte de la persona obligada) de resguardar dichos datos y guardar secreto.
2. Conservación y revelación parcial rápidas de los datos relativos al tráfico (art. 17 del CBC): por un lado, busca garantizar la conservación rápida de datos relativos al tráfico, con independencia a la cantidad de proveedores que hayan tenido participación en el proceso de comunicación; por otro lado busca garantizar la revelación rápida a una autoridad competente del Estado parte de la Convención, o a la persona por él designada, de datos relativos al tráfico en un volumen que resulte suficiente a los efectos de identificar tanto a los proveedores de servicios como a las vías de comunicación por las que se produjo la transmisión de la comunicación.
3. Orden de presentación (art. 18 de la CBC): este recurso permite a la autoridad designada ordenar a una persona que se encuentre en su territorio a que presente determinados datos informáticos, que obren en su poder o se encuentre bajo su control, y se encuentren almacenados en un sistema informático o en un dispositivo de almacenamiento de datos. También permite a la autoridad designada obligar a un proveedor de servicios que opere en su territorio nacional, a que presente datos que obren en su poder o bajo su control, relativos a los abonados en relación a dichos servicios.
4. Registro y confiscación de datos informáticos almacenados (art. 19 CBC): Permite el acceso del investigador de un Estado parte a todo dispositivo de

ISSN/ISSN-L: 3006-2667

almacenamiento de datos o sistemas informáticos, que contengan datos informáticos almacenados en su territorio. Esta modalidad permite incautar o confiscar los datos informáticos almacenados; realizar copias de los datos y conservarlos; preservar íntegramente los datos informáticos; hacer inaccesibles o suprimir los datos informáticos almacenados. También se faculta a ordenar a toda persona que conozca el funcionamiento de un sistema informático, o las medidas adoptadas para la protección de los datos, a que proporcione toda la información necesaria, dentro de lo razonable, para el cumplimiento de los fines previstos en el presente artículo.

5. Obtención en tiempo real de datos relativos al tráfico (art. 20 CBC): Esta procedimiento permite al investigador obtener y grabar en tiempo real datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A tal efecto, incluso es posible obligar a cualquier proveedor de servicios, dentro de sus capacidades técnicas, obtener y grabar los datos mencionados precedentemente. La CBC obliga a los Estados parte a adoptar las medidas legislativas necesarias para incorporar estas facultades a su ordenamiento interno, y para obligar a los proveedores de servicio a mantener la reserva sobre el empleo de estas técnicas.
6. Interceptación de datos relativos al contenido (art. 21 CBC): Esta técnica permite al Estado parte obtener y grabar en tiempo real datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. Se faculta a obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a obtener y grabar los datos requeridos. Es de resaltar, que para el empleo de esta técnica de investigación, el Estado parte deberá confeccionar un listado de Delitos Graves, conforme a su derecho interno, que serán objeto de investigación mediante este mecanismo, no pudiendo generalizarse su utilización a otros delitos. Se faculta además a los Estados partes a obligar a los proveedores de servicio a mantener el secreto sobre el empleo de estas técnicas.

Las técnicas de investigación (o poderes procesales de investigación), incorporados en la CBC constituyen herramientas indispensables a los efectos de la lucha contra la delincuencia en el entorno de las modernas Tecnologías de la Información y la

ISSN/ISSN-L: 3006-2667

Comunicación[12]. La irrupción tecnológica ha otorgado nuevas ventajas a la actividad delictiva, y al mismo tiempo ha levantado desafíos a las fuerzas del orden en múltiples aspectos, uno de ellos referido a las técnicas de investigación apropiadas que deben ser desenvueltas a los efectos de la lucha contra el crimen en estos nuevos entornos.

Importancia de las modernas técnicas de investigación tecnológicas en la lucha contra el crimen organizado

Las técnicas de investigación incorporadas a partir de la adopción de la Convención de Budapest resultan indispensables para otorgar mayor eficacia a la lucha contra la delincuencia organizada. Medidas como el registro y confiscación de datos informáticos, que responden a lo que en doctrina se conoce como el "allanamiento informático", permiten al investigador conocer la información contenida en la memoria de los dispositivos de almacenamiento de datos de personas sospechosas, a partir de la inoculación de virus informáticos especialmente diseñados para el empleo de las fuerzas del orden, remitidos al sospechoso a través de correos spam, correos institucionales, o físicamente a través de dispositivos como pendrives, que se insertan en los dispositivos del sospechoso. Estos virus, por lo general del tipo "troyanos", se encargan de buscar información específica en la memoria de los dispositivos infectados, y de remitir la información seleccionada al investigador, todo ello en un marco de secreto, para no levantar sospecha en la persona investigada. Tal herramienta de información permitiría ahorrar al investigador, y al Estado, tanto en términos de tiempo, como de recursos humanos y materiales, con resultados mucho más enriquecedores para la investigación, al tiempo de evitar poner en riesgo a agentes operativos, con operaciones encubiertas.
El beneficio de la incorporación y el empleo de este tipo de técnicas se proyecta no sólo respecto a la posibilidad de realizar investigaciones en tiempo real, sobre las actividades y operaciones de las organizaciones criminales, sino también sobre la posibilidad de tener un panorama más claro respecto a las fuentes de financiamiento de las operaciones ilegales, el mecanismo empleado para la recaudación, y sobre todo los procedimientos para el lavado de activos de la organización. Esto es así debido a que constituye un

[12] En adelante TIC´s, por sus siglas.

ISSN/ISSN-L: 3006-2667

comportamiento profundamente normalizado en las personas de nuestro tiempo el portar teléfonos celulares, la mayoría de los cuales son verdaderas computadoras (en especial los teléfonos de alta gama), con un gran poder de cómputo y cada vez con mayor capacidad de memoria. Estos artefactos van registrando, de forma directa o indirecta, ya sea con la plena conciencia de su usuario o sin ella, los movimientos, llamados, viajes, y demás tipos de actividades de realiza quien los porta, además de las personas con las que permanece en contacto, información sumamente relevante que cualquier analista podría utilizar para extraer importantes inferencias.

Los recursos antes señalados, aportados por la CBC, suponen la incorporación de herramientas sumamente eficaces, pero que al mismo tiempo deben necesariamente ser objeto de regulación por parte del legislador, debido a la forma en que operan, produciendo injerencias directas en la esfera de los derechos y garantías constitucionales. La ausencia de regulación de estas técnicas supone un problema para el objetivo de la persecución penal pública, en cuanto a la investigación y sanción de los hechos punibles de acción penal pública. La experiencia internacional en este sentido[13] señala que este es un contexto en donde los cambios tecnológicos se producen a una velocidad vertiginosa, lo que hace difícil que la legislación brinde respuestas inmediatas a los desafíos que esto produce en el ámbito de la delincuencia. En este último sentido, resulta frecuente que en un primer momento la administración de justicia recurra a modelos jurisprudenciales elaborados en otros países donde estos fenómenos se han producido con anterioridad, elaborando una suerte de estándares amigables con el empleo de tecnologías modernas en la investigación penal, como un primer paso, para dar luego lugar a las muy necesarias previsiones legislativas que resguarden las garantías constitucionales afectadas por el empleo de estas técnicas de investigación altamente tecnológicas.

Producción y valoración de la prueba informática en el proceso penal

Entendemos que la denominación adecuada es la de "prueba informática" para referirnos a la evidencia que ingresa a través de los medios de investigación antes señalados, ya con miras a su producción en la audiencia de juicio oral y público. El concepto empleado

[13] Brinda referencias al respecto Josefina Quevedo González en su obra INVESTIGACIÓN Y PRUEBA DEL CIBERDELITO, editorial Selpin, Madrid, España, 2017.

ISSN/ISSN-L: 3006-2667

resulta de lo más amplio y abarca a las distintas tecnologías que han surgido, y que seguirán emergiendo posteriormente, en el ámbito de la informática. A este respecto, recordamos que la informática es un área del saber humano que se sustenta sobre otras disciplinas como la física, la matemática, la lógica, y que se refiere al tratamiento automatizado de la información. En tal sentido, las tecnologías conocidas como analógica, y digital, son por tanto nada más que estadios en el desarrollo de la ciencia informática, en la que actualmente se desarrolla otro capítulo más que es la tecnología cuántica. Resulta por tanto técnicamente más adecuado emplear el concepto de "prueba informática" para referirnos a este fenómeno.

El Código Procesal Penal Paraguayo no regula de forma expresa sobre la incorporación, producción y valoración de la prueba informática como categoría específica, le son por tanto aplicables las disposiciones generales sobre la prueba[14]. Rige el principio de libertad probatoria[15]. Por tanto, y de lo anterior, concluimos en que no existe obstáculo alguno para la incorporación de este tipo de pruebas en el contexto del proceso penal.

Ahora bien, la manera en que este tipo de prueba ingresará a juicio debe canalizarse a través de dos medios probatorios tradicionales, que son las documentales y las periciales. El que se emplee uno u otro dependerá exclusivamente de la necesidad de recurrir o no a conocimiento experto en materia informática a los efectos de obtener la información a partir de la extracción de la misma de algún dispositivo de almacenamiento de datos[16], en cuyo caso nos encontraremos ante la necesidad de contar con un perito en materia informática, para que realice la operación conforme a la normativa del CPP. De manera característica se realizan por esta vía la extracción de datos de teléfonos celulares, lo que abarca tantas conversaciones de chats, de distintas aplicaciones; así como del audio de esas conversaciones cuando existiesen. De igual forma, a través de este medio se incorporan los denominados cruces de llamadas (que involucran no solamente la verificación de la conexión entre dos o más números telefónicos, sino además la

[14] Libro Tercero, Medios de Prueba, título I, Normas Generales.

[15] Art. 173 CPP. Libertad Probatoria. Los hechos y circunstancias relacionados con el objeto del procedimiento podrán ser admitidos por cualquier medio de prueba, salvo las excepciones previstas por las leyes. Un medio de prueba será admitido si se refiere, directa o indirectamente, al objeto de la investigación y es útil para el descubrimiento de la verdad. El juez o tribunal limitará los medios de prueba ofrecidos cuando ellos resulten manifiestamente excesivos".

[16] Dispositivo de Almacenamiento de Datos, denominación genérica para todo dispositivo que pueda almacenar datos informáticos como: notebooks; consolas de viodeojuegos; teléfonos celulares; relojes inteligentes; tabletas, etc.

ISSN/ISSN-L: 3006-2667

frecuencia en que se dan tales conexiones, el origen de las llamadas, la duración, fecha y hora de las mismas, elementos muy importantes para establecer patrones de contacto y de relacionamiento entre los usuarios de tales números).

Hay que señalar que en los casos mencionados, el perito realiza las tareas indicadas a partir de los dispositivos previamente incautados con arreglo a la legislación procesal penal y a la ley orgánica del Ministerio Público[17]. Debemos tener presente que el primer desafío para el investigador resulta ser siempre la recolección adecuada de la evidencia incautada, que constituye uno de los aspectos críticos de toda investigación en el contexto de las tecnologías de la información y la comunicación[18]. Actualmente, en Paraguay contamos con dos unidades fiscales especializadas en delitos informáticos, y con el Laboratorio Forense del Ministerio Público, donde se realizan las labores de análisis, extracción de datos, y similares, lo que constituye un avance importante en la materia, dada la creciente importancia de la prueba informática en la investigación penal, que va desplazando inclusive en relevancia a la prueba física[19]. Sin embargo, debemos llamar la atención a la necesidad de que estos organismos cuenten con mayor presupuesto, más personal, y otras facilidades, debido a que el auge del empleo de dispositivos tecnológicos vinculados a la comisión de hechos delictivos en la actualidad corre el riesgo de desbordar las posibilidades de respuesta actuales del Laboratorio Forense y su personal. Por otro lado, las herramientas empleadas en el análisis forense de los dispositivos tecnológicos, como el UFET[20], tienen un significativo costo, que requiere a su vez el pago anual por las licencias y actualizaciones, de tal forma que los recursos económicos disponibles para la investigación permitirán en su caso contar con las herramientas más potentes y actuales, o en caso contrario, determinarán la posibilidad de extraer datos tan sólo de una gama determinada de aparatos no tan modernos ni de alta gama.

De cualquier forma, el momento de la incautación de la evidencia resulta fundamental para evitar el borrado, alteración, y/o contaminación de cualquier manera de la evidencia, para lo cual deben establecerse y seguirse protocolos de actuación estandarizados,

[17] Ley 1.562/2000, Orgánica del Ministerio Público.
[18] En adelante TIC´s.
[19] Al respecto se pronuncia Marcos Salt, en su obra NUEVOS DESAFÍOS DE LA EVIDENCIA DIGITAL: ACCESO TRANSFRONTERIZO Y TÉCNICAS DE ACCESO REMOTO A DATOS INFORMÁTICOS, Ed. Ad Hoc, 1ra. Edición, Buenos Aires, 2017.
[20] Producto de investigación forense para el acceso a datos de teléfonos celulares básicos, smartphones, drones, tarjetas SIM, Tarjetas SD, y otros, elaborado por la firma CELEBRITE.

ISSN/ISSN-L: 3006-2667

obligatorios y verificables a posteriori[21], por las partes involucradas. Asimismo, la cadena de custodia de la evidencia informática requiere necesariamente del empleo de medios técnicos que permitan asegurar la indemnidad de la prueba hasta el momento de su producción ante el Tribunal de Sentencia[22], por lo cual se emplean a este respecto, desde el siglo pasado, algoritmos especiales[23] que transforman la información contenida en los archivos en una cifra alfanumérica de valor constante, cuya utilidad radica en que la aplicación del algoritmo sobre el mismo archivo, en cualquier etapa del proceso penal, debe necesaria e indefectiblemente dar lugar a la misma cifra alfanumérica siempre para establecer la indemnidad de la información. La variación de un solo bit de información del mismo archivo necesariamente dará como resultado una cifra diferente, en cuyo caso la conclusión necesaria será que el archivo fue modificado.

Otro aspecto a tener en cuenta respecto a este tipo de pruebas, es el referido al nivel de injerencia que supone la obtención de la información que el investigador se plantea obtener, para después producir en juicio respecto a la injerencia que ello supone dentro del ámbito de las garantías constitucionales de los afectados. Para clarificar este punto debemos considerar que durante la investigación penal el fiscal debe afrontar obstáculos legales y constitucionales para sus actos de investigación, como lo son indudablemente la existencia de garantías constitucionales como la privacidad[24], o el secreto de las comunicaciones[25]. Ante la necesidad de realizar una acto de investigación que infrinja cualquiera de las garantías constitucionales el fiscal de la causa deberá requerir necesariamente autorización jurisdiccional al Juez o Tribunal competente, quien a su vez deberá expedirse a través de una resolución fundada que exprese los motivos por los cuales la intromisión en el ámbito de las garantías constitucionales resulta razonable, necesaria, útil a los fines del proceso, y proporcional, entre otros aspectos a ser considerados, y finalmente autorizar la intromisión o denegarla.

[21] Sobre este tema se expresa el interesante artículo “La Cadena de Custodia en la Evidencia Digital”, de Gustavo Daniel Presman, en el volumen CIBERCRIMEN II, dirigido por Daniela Dupy, p 303, editorial DdeF, Buenos Aires, Argentina, 2018.

[22] Órgano Jurisdiccional facultado para la valoración de la prueba y la determinación de los hechos en el diseño del proceso penal paraguayo, en la etapa de juicio oral y público, art. 41 CPP.

[23] Confr. “La Cadena de custodia en la Evidencia Digital”, antes citado. Entre los algoritmos más utilizados con la finalidad descripta se encuentran el hash sha256, el hash md5, y otros similares.

[24] Art. 33 CN. Del Derecho a la Intimidad.

[25] Art. 36 CN. Del Derecho a la Inviolabilidad del Patrimonio Documental y de la Comunicación Privada.

ISSN/ISSN-L: 3006-2667

Ingresarán a juicio como documental datos e informaciones que no requieran de la intervención de un experto en materia informática para su obtención, es decir, de la realización de una pericia, lo que no significa que en determinadas circunstancias no deba recurrirse a una autorización jurisdiccional para su obtención. Al respecto, son muchos los datos que las ISP[26] pueden facilitar en el marco de una investigación penal y que posteriormente pueden ingresar como documentales, como ser los datos de abonado, que dan cuenta de la identidad de un determinado usuario del servicio, su domicilio, documento, número telefónico, así como el tipo de servicio prestado, la frecuencia, aparatos facilitados al mismo, y otros datos. Hasta la fecha los tribunales entienden que el requerimiento de este tipo de datos puede realizarlo exclusivamente el Fiscal a cargo de una investigación penal en curso, sin que se requiera autorización jurisdiccional al respecto, ya que no se vulnera con ello el ámbito de la intimidad o el secreto de las comunicaciones[27]. Es más problemático a este respecto el requerimiento de datos de tráfico o metadatos[28], los que si bien no se refieren al "contenido" de la comunicación, configuran datos propios de un registro sobre la comunicación, para algunos abarcado por la protección del texto constitucional en el art. 36, Del Derecho a la Inviolabilidad del Patrimonio Documental y de la Comunicación Privada[29].

Ingresarán también como documentales otros datos remitidos por las ISP, como ser el informe sobre la ubicación georreferenciada de los teléfonos obtenidos a través de las celdas de telefonía celular o CSLI (Cell Site location information)[30]. Estos datos se

[26] Siglas en inglés de Internet Service Provider (proveedor de servicios de internet), denominación de aquellas empresas que gestionan servicios relacionados con internet, y entre ellos especialmente comunicaciones.

[27] Este entendimiento se basa en un estándar elaborado por la doctrina estadounidense conocida como "la doctrina de terceros", que señala que aquellos datos que se dieron a conocer a terceros no se encuentran amparados por la 4ta. Enmienda de la constitución estadounidense, y por lo tanto, no son de carácter privado, ya que no existe al respecto una razonable expectativa de privacidad. En la actualidad nuevos desarrollos jurisprudenciales de la propia Corte Suprema de Justicia Federal de los EE.UU. parecen elaborar otro tipo de interpretación al respecto (confrontar al respecto la obra de Hernán Blanco, TECNOLOGÍA INFORMÁTICA E INVESTIGACIÓN CRIMINAL, La Ley, Thomson Reuters, 1ra. Edición, Buenos Aires, Argentina, 2020, capítulo 5).

[28] "Datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente", art. 1ro, literal "d", Convenio de Budapest, ratificado por Ley 5994/2017.

[29] Dice: "El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica… (…) …no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial…", art. 36, CN.

[30] Confr. Blanco, Hernán, TECNOLOGÍA INFORMÁTICA E INVESTIGACIÓN CRIMINAL, p 164 y siguientes.

ISSN/ISSN-L: 3006-2667

encuentran registrados en las compañías de telefonía celular debido a que las antenas monitorean 24 horas al día, 7 días a la semana, la ubicación de los teléfonos celulares, y pueden ser requeridos sin la necesidad de una pericia, ni autorización jurisdiccional, sin embargo y no obstante, cuando el informe se refiere a un tiempo prolongado respecto al mismo sujeto o a las mismas personas investigadas, corresponde preguntarse si dicha información vulnera o no la intimidad de las personas. Sobre este último aspecto, la Suprema Corte de Justicia de los EE.UU., en el precedente "Carpenter Vs. Unitet States", se pronunció respecto a un caso vinculado a la obtención de datos de tráfico, vinculado a la obtención de datos de CSLI. La policía había recolectado este tipo de datos vinculados a los movimientos de dos personas investigadas, a fin de reconstruir sus movimientos, en un caso donde se las tenía imputadas por un cargo de robo, para el efecto se recabaron datos durante 88 días en un caso y por 127 días en otro. A este respecto, la Corte anuló la evidencia, en un voto dividido, concluyendo que no era aplicable al caso la denominada "doctrina de terceros", cuando se trataba de un monitoreo a largo plazo, debido a que este mecanismo de investigación permitía recopilar una enorme cantidad de información sobre las personas vigiladas, y en el entendimiento de la mayoría, infringía la razonable expectativa de privacidad (estándar legal para determinar la afectación a la 4ta. Enmienda de la Constitución Estadounidense), de los ciudadanos.

Incluso algunos datos podrán ingresar a través de una testifical, como por ejemplo el dato sobre el empleo habitual por parte de una persona de un dispositivo en cuestión, la utilización de un teléfono, o número telefónico, e inclusivo el empleo habitual de una cuenta de una red social, lo que puede constituir un indicio importante en la determinación de la autoría de una conducta punible. En este ámbito resulta fundamental el empleo de la valoración por el sistema de indicios y presunciones, con respecto a la atribución de un hecho a un sospechoso, lo que suele ser una parte sumamente dificultosa de la construcción de la teoría del caso de la acusación.

En lo que respecta a la valoración de la prueba por parte del Tribunal, se requerirá de un primer examen de licitud sobre la prueba[31], que abarcará el análisis respecto a la forma de obtención de la prueba, el respeto a los protocolos de incorporación de la evidencia, la

[31] En este punto seguiremos la argumentación expuesta por Josefina Quevedo González, en su obra INVESTIGACIÓN Y PRUEBA DEL CIBERDELITO, antes citada, p 228 y ss.

ISSN/ISSN-L: 3006-2667

cadena de custodia, la existencia o no de autorización jurisdiccional donde sea necesaria, básicamente, que no se hayan infringidos derechos fundamentales en su obtención.

En segundo término, será necesario un examen de fiabilidad, lo que implica la corroboración de la autenticidad de la prueba, su indemnidad y su integridad. Esta verificación abarca la determinación de si el material valorado pudo o no ser sometido a algún tipo de manipulación, si el material aportado (la información contenida en los dispositivos de almacenamiento de datos que suelen llegar a juicio como Pendrives, discos compactos, o discos láser, memorias externas, etc.), ha sufrido algún tipo de alteración, o ha llegado de forma íntegra; y finalmente si los datos pudieron ser obtenidos a partir de la utilización de algún tipo de técnicas espurias, todo lo cual implicará finalmente su ineficacia probatoria.

El Tribunal debe ser consciente acerca de la volatilidad de la prueba informática, que finalmente se trata de información contenida en un tipo de soporte físico, información escrita en el lenguaje propio de la informática, el binario (ceros y unos), traducida posteriormente a imágenes, audios, o texto, merced a programas con formatos específicos, requeridos para su reproducción en juicio. La duda sobre la autenticidad, originalidad, indemnidad o integridad de la prueba determinará necesariamente su ineficacia probatoria.

Sin embargo y no obstante, si la prueba informática supera los exámenes antes descriptos, tendrá una fuerza probatoria bastante considerable, fundada en la fortaleza de un saber de carácter científico, considerado como bien fundamentado al estado actual de nuestra cultura, como lo es la ciencia informática, por lo que será factible realizar inferencias inductivas fuertes a partir de dicha información.

Incorporación de las medidas tecnológicas de investigación en la legislación paraguaya

Si bien es cierto el Congreso Paraguayo ha ratificado la CBC, que pasó a integrar el derecho positivo nacional, a la fecha han pasado varios años sin que el legislador nacional haya procedido a brindar un tratamiento adecuado a las disposiciones de la Convención a los efectos de hacer posible su aplicación en la práctica, mediante una ley que regule los poderes procesales de investigación contenidos en la CBC.

ISSN/ISSN-L: 3006-2667

Existen numerosas cuestiones que el legislador nacional debe abordar respecto a las técnicas de investigación incorporadas por la CBC, con miras a armonizar su aplicación con relación a los mandatos constitucionales, en materia de derechos y garantías, como asimismo respecto a los compromisos asumidos por el país en materia de Derechos Humanos, a partir de las convenciones y acuerdos internacionales suscritos por la República.

Debemos recordar a este respecto que aquellas medidas de investigación que generen injerencias en el ámbito de los derechos y garantías de las personas investigadas, deben necesariamente ser objeto de regulación legal, principio al que alude el aforismo latino "nulla coactio sine lege"[32], con vigencia para el ámbito de las medidas cautelares. Indudablemente, las medidas de investigación tecnológicas aportadas por la CBC implican injerencias, de distinto grado, en el ámbito de garantías tales como el derecho a la intimidad (art. 33 de la CN[33]); o el secreto de las comunicaciones (art. 36 de la CN), resultando la más leve aquella que permite la resguardo inmediato de datos de tráfico, y resultando la más grave aquella que permite la intervención de datos de contenido en tiempo real. De todo ello, es posible inferir la necesidad de la adecuada regulación de las medidas de investigación aludidas, desde que el no hacerlo propiciaría grandes arbitrariedades en el empleo de estas nuevas técnicas, arbitrariedades hacia las que el poder político de turno puede verse bastante seducido; pero a la vez pondría al país en la mira de nuevas condenas ante la Corte Interamericana de Derechos Humanos por violaciones a las convenciones y acuerdos que dicho Tribunal Regional se encarga de hacer cumplir.

Entre otros aspectos que deben ser objeto de armonización, reflexión, y regulación meticulosa se encuentran:

1. La determinación del tipo de hecho punible al cual podrán ser aplicadas las medidas de investigación incorporadas por la CBC. Partiendo simplemente del grado de injerencia que cada medida de investigación, de las enunciadas, supone para los derechos y garantías constitucionales, en base al principio de proporcionalidad, no sería factible, y lo señala el texto de la propia CBC, que se

[32] Equivalente a la afirmación "no puede existir coerción sin ley", en el sentido de que cualquier medida cautelar que genere coerción hacia el investigado debe necesariamente estar autorizada a través de una ley.
[33] Constitución Nacional, por sus siglas.

ISSN/ISSN-L: 3006-2667

habiliten todas las medidas para la investigación de cualquier tipo de hecho punible de los previstos en la legislación penal ordinaria, es decir, indistintamente a su gravedad. En este sentido, el legislador debe ser muy cuidadoso al establecer el ámbito de los hechos punibles para el cual sería posible emplear estas medidas de investigación. Habilitar el libre ejercicio de todas las medidas de investigación tecnológicas para la investigación de cualquier tipo de hecho punible, habida cuenta del distinto nivel de injerencia que las mismas poseen respecto a derechos y garantías constitucionales constituye un despropósito, reñido con la proporcionalidad, y con el debido respeto a los mandatos constitucionales.

2. La decisión respecto a la autoridad que resultará competente para decidir sobre el empleo o no de la medida de investigación, o la autorización para su ejercicio, también resulta relevante. El legislador deberá sopesar el nivel de injerencia que cada medida de investigación supone respecto al ámbito de los derechos y garantías constitucionales, a los efectos de establecer si una medida de investigación determinada podrá ser autorizada por un Fiscal, o necesariamente deberá contar con una autorización jurisdiccional para dotar de legalidad al empleo de la técnica de la que se trate.
3. El legislador debe regular las condiciones de modo y tiempo en que serán ejercidas las medidas tecnológicas de investigación, así como las condiciones de control sobre su ejercicio, a los efectos de evitar el empleo abusivo de las mismas en detrimento del libre goce de los derechos y garantías constitucionales. Ninguna medida de investigación puede extenderse sin límites de tiempo, y sin sujetarse a condiciones o requisitos para su ejercicio. Asimismo, las mismas deben permitir el adecuado control a ser ejercido posteriormente por la parte afectada en las oportunidades establecidas en la legislación procesal penal.
4. El legislador debe además regular determinadas condiciones que constituyen requisitos indispensables para el ejercicio efectivo de muchas de las medidas de investigación antes señaladas, como el tiempo que los proveedores de servicio deben estar obligados a guardar los distintos tipos de datos que forman parte del flujo de comunicaciones que pasan por sus infraestructuras. Este aspecto resulta esencial debido a que no se podría disponer para una investigación penal de datos almacenados relevantes, si el propio proveedor de servicios no se encuentra

ISSN/ISSN-L: 3006-2667

obligado a guardarlos durante un tiempo razonable (conforme a los plazos de una investigación penal), lo que provocaría la pérdida de evidencia relevante y podría tornar inútiles muchas investigaciones.

5. Es asimismo relevante que el legislador reglamente los casos de obligación de guardar secreto sobre las medidas empleadas, así como el ámbito de los sujetos afectados por esta obligación. Este aspecto resulta relevante por cuanto de enterarse el afectado sobre la existencia de medidas tecnológicas de investigación dispuestas en su contra el afectado bien podría modificar, alterar, encriptar o destruir los datos que se pretende recabar.

BIBLIOGRAFÍA

Blanco, H. (2020). *Tecnología informática e investigación criminal* (1ra ed.). La Ley.

Chavez Cotrina, J. (2019, octubre 22). *Análisis de acuerdos plenarios 2019 – Técnicas especiales de investigación* [Video]. YouTube. https://www.youtube.com/watch?v=9jQYFLTr_EI

Constitución de la República del Paraguay. (1992).

Garibaldi, G. E. L. (2010). *Las modernas tecnologías de control y de investigación del delito: Su incidencia en el derecho penal y los principios constitucionales* (1ra ed.). Ad-Hoc.

Guanes Nicoli, M. (2022). *El control jurisdiccional de la intervención de las comunicaciones telefónicas*. En G. D. Meirovich & R. Berruezo (Eds.), *Ilícitos económicos y evidencia digital*. IJ Editores.

Ley N° 1340/88, que modifica y actualiza la Ley N° 357/72, que reprime el tráfico ilícito de estupefacientes y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes. (1988).

Ley N° 4788/12, integral contra la trata de personas. (2012). Artículos 23–29.

Ley N° 5994, aprueba la Convención sobre la Ciberdelincuencia, y el protocolo adicional al convenio sobre ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. (2019).

Ley N° 6431/19, que crea el procedimiento especial para la aplicación del comiso, el comiso especial, la privación de beneficios y ganancias y el comiso autónomo. (2019).

ISSN/ISSN-L: 3006-2667

Muñoz Conde, F. (2007). *Valoración de las grabaciones audiovisuales en el proceso penal* (2da ed.). Hammurabi.

Roxin, C. (2008). *La prohibición de autoincriminación y de las escuchas domiciliarias* (1ra ed.). Hammurabi.

Salt, M. (2017). *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos* (1ra ed.). Ad-Hoc.