Ciclo Político de Justicia
compartido entre América Latina y la Unión Europea

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

LA PRUEBA ELECTRÓNICA EN EL MARCO NACIONAL Y EN EL INTERNACIONAL EN LATINOAMÉRICA

Sixto Luque Delgado
Marcos Salt
Carlos Pinho
Pedro Verdelho

Ediciones EL PAcCTO
Colección A Fondo

La prueba electrónica en el marco nacional y en el internacional en Latinoamérica

Sixto Luque Delgado

Marcos Salt

Carlos Pinho

Pedro Verdelho

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Edita: Programa EL PAcCTO
Calle Almansa 105
28040 Madrid (España)
www.elpaccto.eu

Bajo la coordinación de:

FIIAPP

EXPERTISE FRANCE

SIXTO LUQUE DELGADO
Es magistrado del Juzgado de Primera Instancia e Instrucción número 5 de Marbella. Anteriormente fue magistrado del Juzgado de Primera instancia e instrucción de Plasencia (Cáceres), juez titular de los juzgados de primera instancia e instrucción de Cádiz, Málaga, Santa Cruz de Tenerife y Granada, con competencia exclusiva en materia de violencia sobre la mujer. Licenciado en Derecho por la Universidad de Jaén. Ha impartido ponencias en materia de jurisdicción voluntaria y usos y abusos en la asistencia jurídica y gratuita en la jurisdicción civil.

MARCOS SALT
Es abogado especializado en causas penales de la Facultad de Derecho de la Universidad de Buenos Aires, donde es Profesor de Derecho Penal y Procesal Penal. Ha dictado cursos y conferencias en diversas universidades y organizaciones nacionales y extranjeras, y es autor de numerosos artículos científicos sobre su especialidad. Ha sido consultor en delitos informáticos y prueba digital en procesos penales para el Consejo de Europa. Ha sido miembro del Comité de Redacción del Segundo Protocolo Adicional de la Convención de Budapest y de la Comisión encargada de la redacción del proyecto de Ley en materia de delitos informáticos y la adecuación de la legislación argentina a las recomendaciones y convenciones internacionales.

CARLOS PINHO
Es Procurador de la República en el Ministerio Público de Portugal. Es responsable en el área de innovación y proyectos tecnológicos. Miembro del grupo técnico de ciberdelincuencia y experto en evidencia digital y protección de datos informáticos.

PEDRO VERDELHO
Es Procurador de la República en el Ministerio Público de Portugal desde 1990. Director de la Oficina Ciberdelito (Gabinete Cibercrime) de la Procuraduría General de la República portuguesa. Miembro del Comité de Redacción de la Convención sobre Ciberdelito del Consejo de Europa (Convenio de Budapest) y del Comité de Redacción de sus Protocolos Adicionales. Representante de Portugal en el T-CY, el Comité de gestión del Convenio de Budapest desde 2006 - actualmente, vicepresidente del comité. Autor de varios artículos sobre ciberdelito y evidencia digital.

Edición no venal
Madrid, 4 de julio de 2022

Este documento ha sido elaborado con la ayuda financiera de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva del programa EL PAcCTO y, en ningún caso, debe considerarse que refleja el punto de vista de la Unión Europea.

Índice

La prueba electrónica en el marco nacional y en el internacional en Latinoamérica

Prólogo

La sociedad actual tiene muy poco que ver con la que vio nacer la mayor parte de las leyes procesales vigentes. Nuestra vida está monitorizada por las tecnologías de comunicación y dependemos de ellas en cada minuto. Vivimos pegados al teléfono: a través de una pantalla que se guarda en un bolsillo compramos, nos comunicamos, realizamos gestiones de toda clase, no usamos mapas ni preguntamos la dirección, contactamos y nos relacionamos por redes sociales, consultamos la mayor biblioteca del mundo en instantes, etc. La tecnología nos controla y predice nuestro comportamiento al mismo tiempo que resuelve de manera acelerada muchos problemas. Sin embargo, las leyes están pensadas en el papel y en los testimonios.

Los delitos, todos los delitos y no solo el cibercrimen, pueden cometerse mediante tecnologías o bien pueden requerir la incorporación de material probatorio plasmado en formatos electrónicos, desde las conversaciones en un chat a las grabaciones de un robo común tomadas en la vía pública por la cámara de un establecimiento, pasando al contenido de la caja negra de un avión. Los fiscales deben tener la capacidad y la destreza de aportar y los jueces la de valorar.
Nos encontramos ante un trabajo metódico, excelente y novedoso, que parte de la situación vigente con distintos puntos de abordaje y una finalidad muy clara. El enfoque tiene en consideración las definiciones de la prueba, la retención de datos por los proveedores de servicios, las medidas procesales básicas y las técnicas especiales de investigación, tomando como base el estado actual legislativo, las leyes más recientes en la materia y las convenciones internacionales comunes más avanzadas, incluido el Segundo Protocolo al Convenio sobre Cibercrimen de Budapest (2022).

La finalidad es la preparación de una ley modelo sobre la materia, que en la actualidad está en desarrollo en el marco del Ciclo Político de Justicia creado en mayo de 2022 en Bruselas y que agrupa la Asociación Iberoamericana de Ministerios Públicos, la Conferencia de Ministros y Ministras de los Países Iberoamericanos y la Cumbre Judicial Europea, basado en la existencia de estándares jurídicos comunes en ambos lados del Atlántico.

El reto es importante, pero no perdamos las perspectivas de futuro. Las tecnologías de 2021 son avanzadas, pero no están al ritmo de las de 2022. Materias como las medidas sobre criptodivisas, el blockchain o la inteligencia artificial son la realidad del presente y algunos de los campos que deben centrar nuestra atención en el futuro.

Antonio Roma Valdés

Introducción

Este trabajo es el producto de una actividad desarrollada en el marco del proyecto EL PAcCTO[1], con el enfoque en el tema de la obtención de la prueba electrónica en investigaciones de naturaleza criminal. El tema de la prueba electrónica o digital, aunque con frecuencia es asociado exclusivamente al ciberdelito, tiene una aplicación práctica mucho más amplia. Es que la prueba electrónica (y sus medios de incorporación a un proceso penal) y todo lo referido a los nuevos medios de investigación en entornos digitales, hoy resultan fundamentales en casi todas las investigaciones penales, mucho más en casos de delincuencia compleja. No es solamente un tema vinculado a los denominados delitos informáticos, sino que se ha generalizado su utilización en las causas de delitos cometidos por medios informáticos y en general en todas las investigaciones penales de cualquier delito en las que cada día más, resulta de utilidad la correcta obtención de pruebas electrónicas. De hecho, es posible advertir a nivel mundial un paulatino reemplazo de la prueba física por pruebas digitales o electrónicas[2] en todos los procesos penales.

Por estos motivos, el propósito principal de este trabajo es identificar los marcos normativos procesales en esta materia en los países adherentes al proyecto EL PAcCTO[3]. Se pretendió con este ejercicio conocer dichos marcos normativos y compararlos con la regulación internacional a fin de identificar en los países de EL PAcCTO falencias y buenas prácticas con el objetivo de realizar propuestas de trabajo. Hemos tomado como modelo de análisis el estándar del Convenio de Budapest sobre Ciberdelito (del 2001), al cual se han incorporado ya muchos de los países del espacio iberoamericano[4]. Sin perjuicio de ello, hemos analizado también lo referido a las nuevas técnicas de investigación en entornos digitales surgidas en el derecho comparado para hacer frente a los nuevos desafíos que genera el entorno digital (a modo de ejemplo, el anonimato en la navegación o las técnicas de encriptación) para una investigación penal eficiente y respetuosa de las garantías individuales.

El trabajo pretende identificar lagunas legislativas en esta materia, de modo a permitir sugerir iniciativas legislativas, u otras, a las competentes autoridades nacionales de los países participantes.

En paralelo, este análisis legislativo buscó igualmente identificar buenas prácticas en relación con la obtención de pruebas electrónicas o digitales, para poderlas compartir entre los países de la región, sobre todo, con respeto a medidas procesales (medidas clásicas, aplicables al entorno digital y también nuevas y específicas medidas del entorno digital) y a las correspondientes garantías procesales, asociadas a las medidas de investigación.

1 EL PAcCTO es un programa financiado por la Comisión Europea que tiene como objetivo la lucha contra el crimen organizado en Latinoamérica, incidiendo sobre los componentes de cooperación policial, cooperación entre sistemas de justicia y sistemas penitenciarios. Lo lidera la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas, de España y Expertise France. Les apoyan, en su desarrollo, el Instituto Ítalo-Latino Americano, de Italia y el Instituto Camões de Portugal.
2 Cf. A modo de ejemplo, Marcos Salt, “Nuevos Desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto de datos informáticos”, Editorial Ad Hoc, Buenos Aires, 2017, pág. 23
3 Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela.
4 Además de España y Portugal, es el caso de Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay y Perú. Brasil y México se encuentran en el proceso de accesión al Convenio.

Contexto

A fin de completar el análisis e identificar el marco legal referido a la prueba electrónica, se elaboró y distribuyó un cuestionario entre los países adherentes a El PAcCTO. En ese cuestionario se formulaban preguntas de respuesta sencilla, que permitieran identificar mejor el marco legal en cada país.

No todos los países respondieron al cuestionario. Por ese motivo, fue necesario desarrollar trabajo adicional de documentación y agendar reuniones con representantes de algunos países, de modo a poder obtener, por esta otra vía, las respuestas que se buscaban, en particular con Adrián Acosta, funcionario de Interpol (Digital Crime Office), con larga experiencia en casos concretos de esta naturaleza, en toda Latinoamérica – de modo a poder obtener, por esta otra vía, las respuestas que se buscaban.

La prueba electrónica en el marco nacional y en el internacional en Latinoamérica

I. Visión General

El panorama general en Latinoamérica, con respeto a la regulación procesal de los medios de prueba necesarios para la incorporación al proceso de prueba electrónica (elementos de prueba en forma de datos digitales o electrónicos), no es el deseable: la mayoría de los países no desarrollaron, todavía, un marco legal específico a este respecto. Antes bien, utilizan por analogía las normas pensadas para la prueba física. La gran mayoría de los países no tiene normas procesales referidas a la prueba electrónica o, en algunos países, solamente previeron parcialmente el tema con alguna norma referida a la incautación de datos o la intervención de comunicaciones digitales. Aunque muchos países tienen códigos procesales modernos diseñados para reemplazar los viejos sistemas inquisitivos por modelos acusatorios, la necesidad de regular de manera específica un set de medios de prueba pensados para las necesidades de la prueba electrónica no fue correctamente advertida por los legisladores. Ello ha llevado a la necesidad de solucionar innumerables problemas prácticos mediante interpretaciones jurisprudenciales que no siempre han encontrado soluciones adecuadas tanto en términos de eficiencia como de protección de garantías.

Una primera conclusión es que, en general, en toda la región de incidencia del proyecto EL PAcCTO, hay necesidad de trabajar en la reforma de los capítulos dedicados a los medios de prueba para regular adecuadamente los diferentes medios necesarios para la incorporación de prueba electrónica a los procesos penales.
El trabajo puede verse facilitado si tenemos en cuenta que hay ya un buen número de países de Latinoamérica que se incorporaron al Convenio sobre Ciberdelito del Consejo de Europa que requiere que los Estados Parte incorporen en su legislación interna normas de derecho procesal en el ámbito de la prueba electrónica.

Cabe mencionar que existen ya buenos ejemplos puntuales de normas en este territorio. Así ocurre, por ejemplo, en materia de intervención en comunicaciones, medida procesal ya frecuente en Latinoamérica. Por otro lado, hay también buenos ejemplos de adaptación legislativa de las normas clásicas, de los códigos procesales penales, a entorno digital.
En este trabajo se toma como referencia, como marco normativo mínimo, el capítulo de normas procesales del Convenio de Budapest, el único instrumento legislativo internacional en vigor a nivel global. Es a partir del Convenio de Budapest que se van a analizar los distintos aspectos de los regímenes nacionales.

Por otro lado, no se hará análisis puntual y específico de las normas procesales. Aunque, por supuesto, se parta de las leyes nacionales vigentes y algunos proyectos de ley, el objetivo es el de obtener una imagen global de la región, con respeto a los temas de obtención de pruebas digitales.

II. Definiciones legales con respecto a prueba electrónica

Introducción

El crecimiento exponencial de las formas de comunicación digital, asociado con el almacenamiento remoto de datos, ha generado una serie de retos para las autoridades judiciales y de policía criminal, que buscan acceso a datos informáticos específicos, para las investigaciones criminales.

En este contexto, es importante evaluar el tratamiento legal que dan las distintas jurisdicciones en relación con las definiciones, en particular con respecto a las categorías de datos informáticos, así como las condiciones y garantías para el acceso a los datos, que varía considerablemente entre los distintos estados.

Las definiciones legales relativas a la prueba electrónica son un elemento fundamental para considerar en el proceso penal y en la correcta tramitación de los instrumentos de cooperación judicial.

Es importante mencionar que no se espera que las definiciones en esta materia caigan dentro de la precisión de un concepto específico legalmente relevante de prueba electrónica, como una categoría de prueba procesal en sí misma, sujeta a su propio cuerpo normativo. Por el contrario, el enfoque en esta materia, en la mayoría de las jurisdicciones, está vinculado a la definición de los conceptos de datos y sistemas de información.

En algunos de los países de la región, el marco jurídico interno no contiene definiciones legales con respecto a prueba electrónica, razón por la cual es muy importante, en este informe, no solo identificar el estado de la legislación en cada país, sino también establecer criterios que permitan señalar formas de implementar dicha legislación.

Por lo tanto, comenzaremos con la descripción de las definiciones legales utilizando como estándar las normas del Convenio de Budapest.

Asimismo, y apoyados en las conclusiones del Comité de la Convención de Cibercrimen de Consejo de Europa (T-CY), explicaremos brevemente los tipos específicos de datos que se pueden ingresar en cada una de las categorías. Luego analizaremos, con base en este estándar, la situación actual en cada uno de los distintos países, y concluiremos con recomendaciones prácticas para las diferentes situaciones posibles.

El Convenio de Budapest

El estándar internacional en esta materia nos lo proporciona el Convenio de Budapest[5/6], con las siguientes definiciones:

Convenio sobre la Ciberdelincuencia	
Datos informáticos (Artículo 1/b.)	Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función
Sistema informático (Artículo 1/a.)	Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa
Datos de abonado (Artículo 18/3)	Cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y el pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acordó de prestación de servicio
Datos de tráfico (Artículo 1/d.)	Todos los 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
Proveedor de servicios (Artículo 1/c.)	i. Toda la entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo

La importancia de las definiciones para las categorías de datos es subrayada por el hecho de que se trata de definiciones operativas, ya que enmarcan los conceptos técnicos que permiten identificar los datos específicos de cada una de ellas.
Como los datos son recopilados y almacenados por los proveedores de comunicaciones y servicios en línea, es esencial que las definiciones resulten en el marco de los datos específicos que son generados por los usuarios de los servicios.
Cuando sea necesario obtener (por supuesto, de modo procesal válido), los datos necesarios para una determinada investigación de naturaleza penal, las definiciones específicas de datos permiten establecer categorías distintas, con distintos regímenes de obtención, como se verá en el siguiente punto.

5 https://www.coe.int/en/web/cybercrime/the-budapest-convention.
6 Traducción en español: https://rm.coe.int/CoERMPublicCommonSearchServices DisplayDCTMContent?documentId=09000016802fa41c.

Tipos específicos de datos por categoría

El siguiente cuadro incluye los tipos específicos de datos relacionados con las categorías de datos de abonado, tráfico y contenido, que están definidos en el Convenio de Budapest.

Categorías	Tipos de datos
Datos de abonado	1. Nombre completo 2. Nombre personalizado, apodo o nombre de inicio de sesión 3. ID de usuario 4. Números de teléfono 5. Correo electrónico 6. Fecha de nacimiento 7. Copia de DNI o pasaporte 8. Datos de facturación / Medios de pago 9. Fecha de inicio y finalización de la cuenta 10. Estado de la cuenta 11. Dirección IP de registro, incluidas fecha/hora 12. Dispositivos associados (incluído ID de dispositivo, IMEI, MAC) 13. Dirección y UDID cuando esté disponible) 14. Tipo de registro, copia de contrato, medio de verificación de identidad al momento del registro 15. Copias de documentos proporcionados por el suscriptor
Datos de tráfico	1. Registros de direcciones IP, incluidas fecha/hora 2. Registros de mensajes y registros de chat 3. Registro de actividad / archivos de registro, incluidas fecha / hora 4. Información de enrutamiento (dirección IP de origen, dirección IP de destino, número de puerto, navegador, encabezado de correo electrónico, ID de mensaje, volumen de transferencia de datos, origen o destino de cualquier mensaje electrónico enviado o recibido de la cuenta) 5. ID de la estación base, incluida la información geográfica y los datos de geolocalización
Datos de contenido	1. Contactos 2. Mensajes 3. Publicaciones 4. Archivos multimedia: videos, fotos, documentos 5. Fotos de perfil 6. Descarga de caja de correo electrónico 7. Descarga de contenido del dispositivo

Definiciones por país

En este apartado presentaremos, por categorías, las definiciones legales en materia de prueba digital en los distintos países.

Estos datos fueron recogidos de acuerdo con el análisis legal y la respuesta de los distintos países al cuestionario elaborado.

País	Definición de datos informáticos	
	Marco Normativo	Definición
Argentina	Ley N.º 27.411 promulgada en 14/12/2017	Toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función
Panamá	Ley 79 de 22 de octubre de 2013 que aprueba el Convenio de Budapest	Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función
Paraguay	Ley N.º 4439 que modifica y amplía varios artículos de la Ley N.º 1160/97 (Código Penal)	Aquellos que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible

País	Definición de sistema informático	
	Marco Normativo	Definición
Argentina	Ley N.º 27.411 promulgada en 14/12/2017	Todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos
Panamá	Ley N.º 79 de 22 de octubre de 2013 que aprueba el Convenio de Budapest	Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa
Paraguay	Ley N.º 4439 que modifica y amplia varios artículos de la Ley N.º 1160/97 (Código penal)	Todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento de datos por medio de un programa informático

País	Definición de datos de abonado	
	Marco Normativo	Definición
PanamáC	Ley N.º 79 de 22 de octubre de 2013 que aprueba el Convenio de Budapest	ualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido

País	Definición de datos de tráfico	
	Marco Normativo	Definición
Argentina	Ley N.º 27.411 promulgada en 14/12/2017	Todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente
Panamá	Ley N.º 79 de 22 de octubre de 2013 que aprueba el Convenio de Budapest	Todos los 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.

País	Definición de proveedor de servicios	
	Marco Normativo	Definición
Panamá	Ley N.º 79 de 22 de octubre de 2013 que aprueba el Convenio de Budapest	Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo

Proyectos legislativos en materia de definiciones de categorías de datos

País	Proyecto Legislativo
Brasil	PLC 5441/2020
Chile	Proyecto de Ley, Boletín N.º 12.192-25

III. Retención de datos por los proveedores de servicios

La retención de datos informáticos se refiere a una obligación legal o reglamentaria general impuesta a los proveedores de servicios de comunicaciones electrónicas de retener, por un plazo determinado en meses o años, todos los datos de abonado y de tráfico de todos sus clientes **y sin necesidad de causa penal concreta**, a fin de que oportunamente, y conforme a los requisitos que la ley establezca, sean cedidos a las autoridades judiciales del país en cuestión. Esta medida, al estar regulada por ley, suele tener estándar de obligación, y debe ser cumplida por todos los proveedores. En general, las normas de retención de datos están previstos en leyes que regulan las telecomunicaciones y no en los CPP.

El Convenio de Budapest, en su lugar, reguló la orden de conservación como medida cautelar a fin de solicitar que los proveedores conserven los datos informáticos por un plazo determinado y para una investigación penal concreta (no con carácter general sino vinculado a una causa penal concreta), que cobra relevancia primaria ante la ausencia de obligación general de retención de datos en muchos países. En otras palabras, cuando los proveedores de servicios no tengan una obligación general de retención de datos, muy probablemente guarden la información a fin de ser cedida posteriormente a los órganos de persecución penal, únicamente según su política interna y su capacidad técnica. Puede ser que si la orden de conservación demora, el proveedor ya haya borrado la información.

Cuando se redactó el Convenio de Budapest, sus redactores dejaron constancia en el Informe Explicativo del dilema sobre la conveniencia de regular una obligación general de retención de datos o si regular la orden de conservación, decantándose por esta última.[7]

En lo que respecta a la validez de la obligación general de retención de datos, su validez fue puesta en duda en varios países. En lo que respecta al derecho de la Unión Europea, la obligación estaba regulada mediante la Directiva 2006/24/CE y por un plazo de seis meses a dos años. La directiva fue trasladada al derecho interno de los diferentes países obligados. En el año 2014 el TJUE declaró la invalidez de la Directiva (asuntos acumulados C-293/12 y C-594/12, “Digital Rights Ireland y Seitlinger y otros”), por entender que la imposición de retener datos y permitir el acceso a las autoridades nacionales competentes constituía una intromisión especialmente grave en los derechos al respeto a la vida privada y a la protección de datos personales, reconocidos ambos en la Carta Europea de Derechos Fundamentales, generando un sentimiento de vigilancia constante en sus ciudadanos.

Asimismo, y como argumentos centrales, el TJUE añadió que la reglamentación era insuficiente, no garantizaba que la injerencia en esos derechos se limitara a lo estrictamente necesario, otorgaba facultades de retención muy amplias sin limitaciones en su objeto, no tenía régimen de excepciones, pese a perseguir el interés general de luchar contra delincuencia, infringía el principio de proporcionalidad, no contenía garantías suficientes contra riesgos de abuso y/o acceso y utilización ilícitos de los datos de tráfico, no había criterios sobre cuándo utilizar el plazo mínimo o máximo, remitía a que “serán usados para delitos graves” sin pautas de interpretación, y que los datos retenidos permitían conocer

7 Informe explicativo Convenio de Budapest. El término "conservación de datos" debe distinguirse de la " retención de datos". Si bien ambas expresiones tienen significados similares en el lenguaje común, tienen distintos significados en relación con el uso de los ordenadores. Conservar los datos significa guardar los datos, que ya están almacenados de algún modo, protegiéndolos contra cualquier cosa que pudiera causar una modificación o deterioro de su calidad o condición actual. Retener datos significa guardar a partir de este momento los datos que están siendo generados en este momento. La retención de los datos implica acumular datos en el presente y guardarlos o mantener su posesión en el futuro. La retención de los datos es el proceso de almacenar datos. Por el contrario, la conservación de los datos es la actividad destinada a guardar los datos almacenados de manera segura. Los Artículos 16 y 17 se refieren únicamente a la conservación de datos, y no a la retención de datos. No imponen la obtención y retención de todos, ni incluso de algunos, de los datos recopilados por un proveedor de servicios u otra entidad en el curso de sus actividades. Las medidas referentes a la conservación se aplican a los datos informáticos que "han sido almacenados por medio de un sistema informático”, lo que supone que los datos ya existen, se han obtenido y están almacenados. Además, cuando una Parte emite una orden en que solicita medidas de conservación, esta debe ser en relación a "determinados datos informáticos almacenados que se encuentren en poder o bajo el control de esa persona” (párrafo 2). Por consiguiente, los artículos prevén solo la facultad de exigir la conservación de datos almacenados existentes, quedando pendiente la posterior revelación de los datos en consideración de otras facultades jurídicas, en relación con investigaciones o procedimientos penales específicos.

con mucha precisión con qué persona y de qué modo se comunicaba un usuario registrado, la duración de esa comunicación, la ubicación de los usuarios y hasta la frecuencia en la que se comunican. Por ende, era la regulación contraria al art. 8 del Convenio Europeo de Derechos Humanos.

Previamente, los tribunales constitucionales de varios países habían invalidado por similares motivos las normas nacionales aprobadas en cumplimiento de la Directiva 2006/24 CE. Así a modo de ejemplo, Alemania y Rumania.

Luego, en los Asuntos acumulados C-2013/15 Tele2 Sverige y C-698/15 Secretary of State for the Home Department. Diciembre 2016, el TJUE arribó a conclusiones similares, agregando como argumento que el Derecho de la Unión se opone a una retención generalizada e indiferenciada de los datos de tráfico y de localización, pero que los estados miembros podrán establecer, con carácter preventivo, una conservación selectiva de esos datos con la única finalidad de luchar contra la delincuencia grave, siempre que tal conservación se limite a lo estrictamente necesario por lo que se refiere a las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido. Además, agrega el Tribunal que el acceso de las autoridades nacionales a los datos conservados debe estar sujeto a requisitos, entre los que se encuentran en particular un control previo por una autoridad independiente y la conservación de los datos en el territorio de la Unión.

A continuación, veremos soberamente la regulación en los países miembros de EL PAcCTO que poseen regulada la medida de la retención general de datos en sus legislaciones internas.

Argentina

Argentina reguló la medida de retención general de datos mediante la sanción de la Ley 25873 de diciembre de 2003 modificatoria de la Ley de Telecomunicaciones, mediante la cual se estableció que Los prestadores de servicios de telecomunicaciones deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información debía ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años.

Como puede verse, la disposición obligaba la retención de datos de abonado y de tráfico de las comunicaciones, por un plazo de diez años. Luego, el Decreto 1563/2004 reglamentó la disposición, estableciendo que los operadores debían dar acceso a los datos contractuales actualizados que con relación a sus clientes posean, inclusive la ubicación geográfica y demás datos respecto de los abonados, incluyendo la ubicación geográfica exacta de abonados públicos y semipúblicos. Además, que los licenciatarios de servicios de telecomunicaciones deben arbitrar los medios técnicos y humanos necesarios para que la información esté disponible de inmediato, a toda hora y todos los días del año. Los requerimientos serán realizados por el órgano del estado encargado de ejecutar las interceptaciones en el marco de la legislación vigente y con sustento en las normas que establece la Ley Nº 25.520 y su reglamentación.

Conforme al texto de la citada ley, para dar respuesta a los requerimientos aludidos, los licenciatarios debían establecer mecanismos que permitieran la inmediatez de su respuesta. A tal fin, los pedidos y sus contestaciones podrán ser canalizados a través de medios electrónicos u otros medios fehacientes, siempre que guarden la debida tutela de la información, y en tanto resulten idóneos conforme a la celeridad y certeza que la tarea exige.

Los licenciatarios de servicios de telecomunicaciones debían conservar los datos filiatorios de sus clientes y los registros originales correspondientes a la demás información asociada a las telecomunicaciones, por el término de DIEZ (10) años.

Esta reglamentación fue suspendida mediante Decreto 357/2005 luego de una importante repercusión mediática contraria a la ley en los medios masivos de comunicación.
Asimismo, la ley fue declarada inconstitucional en el año 2009 por la Sentencia Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986.

Entre los argumentos destacables del fallo de la CSJN, se establecieron que todas las comunicaciones aludidas por la ley integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los art. 18 y 19 de la Constitución Nacional, y que por ende se transgredían dichas disposiciones constitucionales. Asimismo, la medida había sido regulada con extrema vaguedad ya que no resultaba claro en qué medida podían las prestatarias captar el contenido de las comunicaciones sin la debida autorización judicial, y, tal como está redactada la norma, existe el riesgo de que los datos sean utilizados para fines distintos que aquellos en ella previstos. Asimismo, el fallo señaló la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales.

Por último, la resolución de la CSJN argumentó que las previsiones de la Ley no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Por ende, la sentencia considera que los datos de tráfico de comunicaciones merecen un estándar de protección tan elevado como los propios datos de contenido de las comunicaciones.

Brasil

El art. 13 de la Ley 12.965 del 23 de abril de 2014 denominada “Ley que establece principios, garantías, derechos y deberes para el uso de Internet en Brasil” establece una obligación de retención aplicable al administrador del sistema relativo a todos los registros de conexión, con confidencialidad, en un ambiente seguro, por el período de un año.

El art. 5.6 dice que estos registros son la información sobre la fecha y hora de inicio y finalización de una conexión a Internet, su duración y la dirección IP utilizada por el terminal para enviar y recibir paquetes de datos. Por su parte, define al administrador del sistema a la persona natural o jurídica que administra bloques específicos de direcciones IP y el respectivo sistema de enrutamiento autónomo, debidamente registrado ante la entidad nacional responsable del registro y distribución de direcciones IP geográficamente referidas al país.

El art. 13.1 establece que la obligación no puede transferirse a terceros. Luego establece plazos cautelares de conservación por períodos extra, que serán analizados oportunamente al explicar lo relativo a la orden de conservación en el capítulo IV de este trabajo.
El art. 13.5 en lo referido a la entrega de información, establece que la puesta a disposición al solicitante de los registros deberá ir precedida de autorización judicial.
Por último, si se incumplen las obligaciones establecidas en ese artículo, puede haber sanciones por incumplimiento.

El art. 15 establece otra obligación de retención aplicable a los prestadores de aplicaciones de internet, por seis meses, para los registros de acceso a las aplicaciones de Internet. Según el art. 5.7 estos datos son un conjunto de informaciones sobre la fecha y hora de uso de una determinada aplicación de Internet, desde una determinada dirección IP. Respecto

a aplicaciones de internet, la ley las define como un conjunto de funcionalidades a las que se puede acceder a través de un terminal conectado a Internet.

Los datos deben ser retenidos bajo confidencialidad, de forma controlada y con medidas de seguridad.

También se establece que con una orden judicial se podrá obligar, durante un tiempo determinado, a los proveedores que no estén sujetos a esta obligación, a que lleven estos registros de acceso a las aplicaciones, siempre que se relacionen con hechos concretos en un período determinado. Luego se establecen las mismas disposiciones ya comentadas sobre conservación específica por un plazo adicional, y necesidad de orden judicial para el acceso a tales datos.

Chile

El art. 13 de la Ley 12.965 del 23 de abril de 2014 denominada “Ley que establece principios,Chile previó en su CPP, art. 222, la obligación de retención de datos vinculada a la obligación impuesta al sector privado de colaborar en la interceptación de comunicaciones. En la Parte pertinente, el Art. 222 establece: “…Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses, de los números IP de las conexiones que realicen sus abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato...”

En Chile estuvo en discusión el Decreto 866/2017 de Reglamento sobre interceptación de comunicaciones telefónicas y de otras formas de telecomunicación, y de conservación de datos comunicacionales, que se lo conoció mediáticamente como Decreto Espía. Este Decreto establece que, los datos comunicacionales relevantes para el cumplimiento de los cometidos de los órganos del estado deberán conservarse por parte de las empresas prestadoras de servicio y por cualquier persona debidamente individualizada, en carácter de reservado, a disposición del ministerio público y de otra institución que se encuentra facultada por ley para requerirlos.

El decreto establece que los prestadores mantendrán y almacenarán por un período no inferior a dos años, en carácter de reservado y a disposición de la autoridad todos los datos comunicacionales a que se alude en el decreto. Respecto a que datos puntuales deben conservarse, el decreto establece que serán los antecedentes del suscriptor y usuario que permitan conocer los datos administrativos y financieros de los mismos, sea la forma y medios de pago que utiliza, el periodo de habilitación y tipo de servicio, los antecedentes necesarios para identificar el origen de la comunicación, tales como número de teléfono, nombre y datos del suscriptor, direcciones IP, entre otros, los antecedentes necesarios para identificar el destino de la comunicación, fecha hora y duración, clase o tipo de comunicación, equipos terminales intervinientes en la comunicación y su ubicación geográfica, con las indicaciones y requisitos que exige la norma técnica respectiva.

El decreto establece que siempre se deberá resguardar la confidencialidad y seguridad de los datos. Este decreto fue criticado por numerosas organizaciones de Derechos Civiles.

Panamá

La Ley 51 2009 de Panamá relativa a normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones, regula una obligación de retención de datos informáticos. El art. 1 establece que las empresas concesionarias, los distribuidores, los agentes autorizados y los revendedores de telefonía móvil, fija y troncal, los Internet cafés, las infoplazas y las redes de comunicación que presten el servicio y/o lo comercialicen, en o desde la República de Panamá, deberán establecer y conservar un registro de datos que proporcione la identificación y dirección suministradas por los usuarios que contraten sus servicios, en cualquiera de sus modalidades, en todo el territorio nacional.

El art. 2 realiza un detalle minucioso sobre qué tipos de datos son los que deben retenerse para cada categoría de datos de rastreo e identificación del origen de una comunicación, de identificación del destino de una comunicación, de determinación de hora, fecha y duración, tipo de comunicación, el equipo de comunicación, y la localización del equipo o celda.
El art. 3 establece la obligación de retención de los datos en dichas empresas, siempre que sean generados por estas en el marco de la prestación de servicios. La obligación de retención incluye una base de datos sobre equipos móviles hurtados, extraviados, robados o encontrados.

Respecto al plazo de retención, es de seis meses, contados desde la fecha de generación de la información. No obstante, a solicitud de autoridad judicial se puede ampliar el plazo para determinados datos hasta seis meses adicionales, tomando en consideración el costo de almacenamiento y la conservación de los datos, así como el interés para los fines de detención con mi investigación sobre el enjuiciamiento de los delitos.
Agrega la ley que, la obligación de retención no conllevará en ningún caso actividades dirigidas interceptar, grabar o acceder al contenido de las comunicaciones de telefonía fija o móvil, o a la información generada por motivo de las comunicaciones de Internet, así como todo otro uso distinto a los que dispone la ley. Se establece la confidencialidad y deber de protección de la misma.

Respecto a la cesión, la ley establece que es un deber cederlos al Ministerio Público o a la autoridad judicial, guardando reserva. Asimismo, se establece que el Ministerio Público podrá solicitarlos a las empresas mediante resolución motivada con base el principio de proporcionalidad de excepcionalidad, la que será objeto de control o revisión posterior por parte de la autoridad judicial. Respecto al plazo de respuesta de los sujetos obligados, será de cinco días hábiles, y si los datos estuvieran enmarcados en el plazo ampliado de retención que establece la ley, serán 15 días hábiles.

Perú

Perú establece la obligación de retención en el Decreto Legislativo del 2015 que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado. La finalidad del decreto es regular el acceso de la unidad especializada de la policía nacional, en casos de flagrancia delictiva, a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar.

Luego de regular el procedimiento, el Decreto establece una disposición complementaria final segunda que dice que los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros 12 meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real.

Luego regula que, concluido el referido periodo, deberán conservar dichos datos por 24 meses adicionales, en un sistema de almacenamiento electrónico. La entrega de datos almacenados por un periodo no mayor a doce meses se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete días siguientes a la autorización judicial, bajo responsabilidad.

IV. Normas procesales específicas sobre prueba electrónica

En lo que respecta a la implementación de medidas procesales específicas sobre prueba electrónica, un indicador importante a tener en cuenta es la adhesión de los países de la región que integran EL PAcCTO al Convenio para la Ciberdelincuencia del Consejo de Europa (Convención de Budapest). Este instrumento internacional prevé un capítulo específico sobre medidas procesales relacionadas con prueba digital que los estados parte se comprometen a sancionar en su derecho interno, con el objetivo de dotar de herramientas procesales específicas en la investigación de cualquier tipo de delitos que tengan prueba electrónica. Se trata de un “set” de medios de prueba pensados para la prueba en entornos digitales que resulta un piso común básico para tener en cuenta por los países. La regulación a nivel de derecho interno de los diferentes países de estos medios de prueba permite contar con herramientas procesales homogéneas que facilitan tanto la investigación a nivel interno como una mejor cooperación internacional.

En este sentido, resulta importante para este estudio tener en cuenta el estado de adhesión al Convenio de Budapest de los países de la región que integran EL PAcCTO[8]:

8 Estado de adhesión conforme la Oficina de Tratados del Consejo de Europa, accesible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=3wUKCCew
9 Estados observadores del Comité de Convenio de Budapest: https://www.coe.int/en/web/cybercrime/parties-observers

Cabe destacar el importante número de países (la mitad de los países ha trabajado en la adhesión al Convenio) y otro grupo como son los casos por ejemplo de México, El Salvador, Guatemala y Ecuador han participado de las actividades de capacitación y asistencia técnica e, incluso, han elaborado proyectos de ley tomando como modelo las propuestas de la Convención de Budapest.

No obstante, y más allá de adherir a dicho instrumento, son pocos los países que han avanzado en una verdadera implementación del Convenio en lo que se refiere a las normas procesales. Antes bien, aun en los países que cuentan con legislación procesal moderna inspirada en los principios del sistema acusatorio, no se adoptaron normas especiales pensadas para los medios de prueba digital y primó la idea de la aplicación de los medios de prueba tradicionales por analogía y en base a una interpretación amplia de los alcances del principio de libertad probatoria que no permite solucionar todas las cuestiones prácticas y jurídicas que involucra la prueba digital y las investigaciones en entornos digitales.
Por esta y otras razones, cuantitativamente son pocos los países miembros de EL PAcCTO que cuentan con legislación específica en materia de normas procesales penales que prevean de manera especial medios de prueba adaptados a las necesidades que plantea la prueba digital.

Así, los códigosz revisados no prevén un conjunto de normas que establezcan con claridad los poderes procesales pensados para el paradigma de la prueba digital como el aseguramiento de datos, orden de presentación, registro y secuestro de datos informáticos, intervención en tiempo real de datos de tráfico y datos de contenido, etc. Antes bien, existe una tendencia a aplicar las tradicionales normas sobre pruebas pensadas para la evidencia física por analogía, en virtud de lo que se denomina principio de libertad probatoria en materia procesal, presente en casi todos los Códigos Procesales de la región. Este uso del principio de “libertad probatoria”, más allá de sus posibilidades, puede afectar tanto la eficiencia de las investigaciones como la vigencia de garantías individuales.
A continuación, haremos una reseña del estado de la legislación en materia de prueba electrónica de los países miembro de EL PAcCTO.

País	Ratificación	Entrada en vigor
Argentina	5/6/2018	10/01/2018
Bolivia	-	-
Brasil	Invitado a acceder. La invitación expira en mayo 2022	
Chile	20/04/2017	01/08/2017
Colombia	16/03/2020	01/07/2020
Costa Rica	22/09/2017	01/01/2018
Cuba	-	-
Ecuador	-	-
El Salvador	-	-
Guatemala	Invitado a acceder. La invitación expira en abril 2025	
Honduras	-	-
México	País observador[9]	
Nicaragua	-	-
Panamá	05/03/2014	01/07/2014
Paraguay	30/07/2018	01/11/2018
Perú	30/07/2018	01/11/2018
Uruguay	-	-

Primera parte: medidas procesales básicas sobre prueba digital

Tomamos como modelo de análisis las medidas propuestas por la Convención de Budapest

Estado de implementación medidas procesales Convenio de Budapest

País/Artículo	Art. 16	Art. 17	Art. 18	Art. 19	Art. 20	Art. 21
Argentina	-	-	-	SÍ[10]	SÍ[11]	SÍ[12]
Bolivia	-	-	-	-	-	-
Brasil	SÍ	SÍ	SÍ	-	SÍ	SÍ
Chile	-	-	-	-	-	-
Colombia	-	-	-	SÍ	SÍ	SÍ
Costa Rica	-	-	-	-	SÍ	SÍ
Cuba	-	-	-	-	-	-
Ecuador	-	-	-	-	SÍ	SÍ
El Salvador	-	-	-	-	-	-
Guatemala	-	-	-	-	-	-
Honduras	-	-	-	-	SÍ	SÍ
México	-	-	-	SÍ	-	SÍ
Nicaragua	-	-	-	-	-	SÍ
Panamá	-	-	-	SÍ	-	SÍ
Paraguay	-	-	-	-	-	-
Perú	-	SÍ	-	-	SÍ	SÍ
Uruguay	-	-	-	-	-	SÍ

10 Art. 144 del Código Procesal Penal Federal en implementación.
11 Art. 143 del Código Procesal Penal Federal en implementación.
12 Art. 143 del Código Procesal Penal Federal en implementación.

Argentina

Argentina es parte del Convenio de Budapest desde el año 2017 mediante la sanción de la Ley 27411. En lo que refiere a la prueba digital no posee un catálogo de reglas procesales específicas que regulen los medios de prueba digital en el Código Procesal Penal de la Nación vigente en gran parte del país ni en el nuevo Código Procesal Penal Federal en etapa de implementación.

Cabe resaltar para una mejor comprensión que Argentina es un país federal. Esto implica que, además del gobierno federal, el país está dividido en 23 jurisdicciones provinciales y una ciudad autónoma que oficia de capital del gobierno federal. Cada una de estas jurisdicciones posee su respectiva administración de justicia, conforme indican los arts. 5 y 123 de la Constitución Nacional, así como la posibilidad del dictar leyes (poder constituyente)[13], entre otras competencias. Esas leyes refieren, entre otras materias, a la organización y administración de la justicia.

Por ende en Argentina, y en lo que refiere a la normativa procesal penal, coexisten los Códigos Procesales Penales de las 23 provincias y de la Ciudad Autónoma de Buenos Aires, así como el Código Procesal Penal Federal, de aplicación para aquellos delitos que no sean de juzgamiento por las jurisdicciones provinciales ordinarias, reservándose su aplicación para la investigación de delitos por parte de la justicia del gobierno federal con asiento en las provincias y en la Ciudad Autónoma de Buenos Aires.

No obstante, por imperio del art. 75 inc.12 de la Constitución Nacional, el Código Penal solamente puede ser dictado por el parlamento del gobierno federal, por lo que solamente hay un único cuerpo normativo de delitos.

Esto quiere decir que el presente análisis girará especialmente en torno a la normativa procesal penal federal, no obstante realizar consideraciones de algunos códigos de las provincias.

El nuevo Código Procesal Penal Federal, el cual se encuentra actualmente en implementación y que reemplazará progresivamente al CPP de la Nación, sí posee algunas disposiciones incompletas relativas a la prueba digital.

Asimismo, en algunos de los códigos procesal penales vigentes en las provincias para el tratamiento de delitos no federales como consecuencia del ya mencionado sistema federal se han regulado algunas normas referidas a la prueba digital. A modo de ejemplo, las normas de los CPP de las provincias de Salta, Neuquén, Tucumán y, más reciente, Corrientes que incluye también normas especiales de investigación tecnológica.[14]

En el Código Procesal Penal de la Nación todavía vigente para las causas que tramitan en el fuero federal (salvo en los lugares en los que el nuevo CPP federal ya está implementado), las disposiciones adjetivas están pensadas para la evidencia física y se aplican a los medios de prueba digital con basamento en el denominado principio de libertad probatoria[15] con las

13 BIDART CAMPOS, Germán “Manual de la constitución Reformada – Tomo 1”, 2006, Editorial Ediar, pág. 386.
14 Por ejemplo, el Código Procesal Penal de la Provincia de Neuquén ya menciona en el art. 150 la posibilidad de obtenerse aun en tiempo real, los datos de tráfico de las comunicaciones
transmitidas por un sistema informático y también el contenido de las mismas, así como orden presentación y registro y secuestro de datos en el art. 153. El Código de la Provincia de Corrientes que en los arts. 180 y ss. regula la interceptación de correspondencia e incautación de datos informáticos, e incluso la vigilancia remota sobre equipos informáticos, en el art. 217, o 196 y ss. del Código Procesal Penal de Tucumán.
15 El principio de libertad probatoria está regulado en el art. 127 del Código Procesal Penal Federal, que establece que podrán probarse los hechos y circunstancias de interés para la solución correcta del caso, por cualquier medio de prueba, salvo que se encuentren expresamente prohibidos por la ley. Además de los medios de prueba establecidos en el Código se podrán utilizar otros, siempre que no vulneren derechos o garantías constitucionales y no obstaculicen el control de la prueba por los demás intervinientes.
La mayoría de los Códigos procesales penales de las provincias también tienen regulado este principio.

dificultades que esto trae tanto en términos de eficiencia como de garantías individuales.[16]

El art. 224 establece que, si hubiere motivo para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito, o que allí puede efectuarse la detención del imputado o de alguna persona evadida o sospechada de criminalidad, el juez ordenará por auto fundado el registro de ese lugar. Como puede verse, posee un sustrato material elevado, dado que en lugar de referir especialmente a evidencia electrónica o trayendo disposiciones específicas en ese sentido, habla de lugares. Asimismo, las disposiciones sobre el modo de ejecución de esta medida y del allanamiento también refieren a la prueba física, dado que por ejemplo menciona que podrá realizarse desde que salga hasta que se ponga el sol.

Respecto al secuestro, el art. 231 establece que el juez podrá disponer el secuestro de las cosas relacionadas con el delito, las sujetas a decomiso o aquellas que puedan servir como medios de prueba. Tampoco refiere explícitamente a la prueba electrónica, dado que no regula la obtención de copias, cadena de custodia, preservación de la integridad, etc., tal como propone el Convenio de Budapest. Nuevamente, por el principio de libertad probatoria, y una interpretación amplia que no siempre es correcta, se utilizan estas medidas pensadas para la prueba física.

Estas disposiciones podrían alcanzar para obtener para el proceso el soporte material donde puede estar alojada la prueba digital, pero no regula ni mínimamente el procedimiento para el acceso a los datos. No obstante, y por una aplicación forzada del principio de libertad probatoria, y ante la ausencia de medias procesales específicas, se suele utilizar esta disposición para lograr su acceso. Por el contrario, si no es esta disposición, suele aplicarse el capítulo referido a peritajes.

La normativa referida a la prueba pericial (art. 253 y subsiguientes) regulan de manera genérica este procedimiento, el cual no refiere a la pericia informática expresamente, sino a cualquier tipo de peritaje técnico. Simplemente regula quién puede ser perito, cuándo se designa, la excusación y recusación, peritos de las partes, dictamen, honorarios, etc.
Pretender aplicar este tipo de medida al registro y secuestro de datos informáticos puede llevar a equívocos y trae innumerables problemas jurisprudenciales. Esto porque la prueba pericial suele ser procedente para que el juzgador pueda responder una duda técnica respecto de hechos o circunstancias, como, por ejemplo: ¿qué auto es el que colisiona primero?, ¿de dónde hacia dónde se disparó el arma homicida?, ¿estaba el imputado con sus facultades mentales disminuidas con la posibilidad de estar sufriendo causales de inimputabilidad?, etc.

En cambio, con los dispositivos electrónicos que se obtienen en el marco de un allanamiento y son secuestrados en su sustrato material, lo que se requiere es acceder a los datos que están dentro del soporte y que, potencialmente, servirán como elementos de prueba para incorporar al proceso. En otras palabras, más que la aclaración de una duda técnica como sucede en los peritajes, es un registro propiamente dicho. Sin embargo, puede requerir de conocimientos técnicos especiales como cuando se busca archivos borrados o se utilizan herramientas de búsqueda por palabras clave o códigos hash, cuestión que no encuentra adecuada regulación en los CPP.
Algunas provincias poseen disposiciones específicas para referirse al registro de los datos

16 Hablamos de dificultades dado que el principio de libertad probatoria no es absoluto y no podría avalar las pruebas obtenidas en violación a garantías constitucionales o prohibidas por la ley (ya sea que la limitación recaiga sobre el objeto de la prueba ─límite absoluto─ o respecto a los órganos, medios o procedimientos probatorios –limitaciones relativas─).
De este modo, el principio de libertad probatoria no puede ser interpretado como una autorización abierta para que el estado haga cualquier cosa en la búsqueda de la verdad, aun cuando actúe bajo la justificación de que el hecho ilícito investigado sea de especial gravedad. Antes bien, el estado no puede utilizar todos los medios de prueba disponibles desde un punto vista fáctico sino solamente aquellos que, además, pueden ser obtenidos e incorporados al proceso conforme a derecho. SERGI, Natalia “Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina”, Informe realizado para Asociación por los Derechos Civiles, febrero 2018, pág. 60.

informáticos insertos en dispositivos de almacenamiento. En este sentido, por ejemplo, el art. 181 del Código Procesal de Corrientes, 199 del Código Procesal Penal de Tucumán, o 153 del Código Procesal Penal de Neuquén.

Respecto a la orden de presentación, el art. 232 establece que el juez podrá ordenar, cuando fuere oportuno, la presentación de los sujetos o documentos. Esta medida tampoco refiere a la materialidad digital de la prueba, dado que en lugar de hacer frente a los datos informáticos como hace el art. 18 del Convenio de Budapest, refiere a documentos. Tampoco hay disposición específica que despeje dudas sobre quién puede solicitar los tipos de datos informáticos relacionados con comunicaciones (datos de abonado, contenido o tráfico).

Sobre intervención de comunicaciones, no hay regulada una disposición específica como propone el Convenio de Budapest en sus arts. 20 y 21 sobre la posibilidad de interceptar datos de contenido y de tráfico en tiempo real sobre comunicaciones informáticas. El art. 236 habla de intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, así como obtener los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él. No obstante, dada la ausencia de requisitos adicionales y especificidad, así como su año de sanción y modificación, no es una medida pensada para lo electrónico como propone el Convenio de Budapest.

Además, el hecho de recurrir a expresiones como comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, o comunicaciones similares, y términos similares a modo de “cajón de sastre” para abarcar cualquier tipo de comunicación pasada, presente y futura, no es suficiente.

Este tipo de expresiones suele estar presente en casi todos los códigos procesales al regular la medida de intervención de comunicaciones. Es insuficiente porque, algunos tipos de tecnologías requieren para su intervención mecanismos mucho más agresivos que otras, y puede no ser suficiente una expresión tan genérica como aquella. Por ejemplo, interceptar una comunicación electrónica cifrada requiere romper el algoritmo de cifrado o realizar el procedimiento mediante algún mecanismo intrusivo que no es correcto pretender hacerlo con expresiones tan genéricas, sin requisitos de legalidad adicionales. Daremos por reproducido este comentario en los análisis de los demás países, cada vez que se mencione una expresión similar en la norma de intervención de comunicaciones.

Un panorama similar respecto del principio de libertad probatoria sucede en el Código Procesal Penal Federal (aprobado, pero aún no vigente en todo el país), normativa que instaura un modelo acusatorio y la cual está actualmente en implementación. Este principio está regulado en el art. 127. No obstante, este código posee algunas disposiciones aplicables a la evidencia electrónica expresamente.

Por ejemplo, al regular el registro de lugares, allanamiento y requisa, incorpora una disposición denominada incautación de datos, para referir al registro y secuestro de datos. Si bien la medida no está exenta de críticas, al menos hace alusión específica a dicho supuesto, no siendo necesario recurrir por analogía a medidas de prueba físicas como ser el capítulo de pericias o de registro de lugares físicos (arts. 161 y subsiguientes). En concreto, el art. 144 dice que el juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de este, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación (…).

A su vez, el art. 150 regula cadena de custodia para asegurar los elementos de prueba.

Respecto a la intervención de comunicaciones el art. 143 dice que (…) el juez podrá ordenar, a petición de parte, la interceptación y secuestro de la correspondencia postal, telegráfica,

electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a este, aunque sea bajo nombre supuesto (…).

Si bien la norma tiene requisitos de legalidad y duración, y menciona comunicaciones electrónicas, al someterla al tamiz de los arts. 20 y 21 del convenio faltan regular algunas cosas para adaptarla al paradigma de la prueba electrónica, como ser el deber de colaboración de los proveedores al cumplir la medida, la obligación de mantener en secreto la medida, interacción con los proveedores de servicio de internet en la ejecución, etc. Si bien el último párrafo del art. 143 dice que las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal, dicha disposición es poco específica, dado que se podría haber regulado cómo colaborar en la ejecución de esta.

Algunas provincias poseen disposiciones específicas relativas a la intervención de datos de tráfico y contenido de comunicaciones informáticas. Por ej. el art. 196 del Código Procesal Penal de Tucumán, o el 216 del Código Procesal Penal de Corrientes, o el 150 del Código Procesal de Neuquén, entre otros.

> ***En conclusión, Argentina es parte del Convenio de Budapest, y si bien tiene algunas medidas como las analizadas, para el resto de las cuestiones sigue aplicando por analogía las disposiciones pensadas para la evidencia física con basamento en el principio de libertad probatoria. Por ende, es recomendable realizar una reforma de la ley procesal a fin de regular los medios de prueba digital. Dado el carácter federal del país, lo mismo debería suceder en las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires, para incorporar estas disposiciones específicas.***

Bolivia

Bolivia no es parte del Convenio de Budapest. En su legislación adjetiva no hay disposiciones que regulen la prueba electrónica de manera específica. Su Código de Procedimiento Penal (Ley 1970) data de 1999 y fue reformado en varias oportunidades, siendo una de las más recientes la reforma del 2019 por Ley 1173 denominada Ley de Abreviación Procesal Penal, cuyo objetivo fue procurar la pronta y oportuna resolución de los conflictos penales, adoptando al efecto, medidas indispensables para profundizar la oralidad, fortalecer la lucha contra la violencia a niñas, niños, adolescentes y mujeres, evitar el retardo procesal y el abuso de la detención preventiva y posibilitar la efectiva tutela judicial de las víctimas.

No obstante, ni en la reforma ni en el resto del Código de Procedimiento Penal hay normativa específica suficiente sobre medios relativos a la prueba electrónica. El art. 231 bis del código, reformado por la mentada ley, establece como un tipo de medida cautelar personal la vigilancia del imputado mediante algún dispositivo electrónico de vigilancia, rastreo o posicionamiento de su ubicación física. Pero más que una medida de prueba es, tal como su naturaleza lo indica, una medida de aseguramiento.

El art. 75 contiene una disposición general que dice que el Ministerio Público requerirá indistintamente la realización de estudios científico - técnicos al Instituto de Investigaciones Forenses – IDIF o al Instituto de Investigaciones Técnico Científicas de la Universidad Policial – IITCUP, para la investigación de delitos o la comprobación de otros hechos mediante orden judicial. No especifica qué tipos de investigaciones o estudios podrían solicitarse y si aplica a medidas tecnológicas.

Las medidas procesales del código que se aplican a la prueba electrónica están pensadas para la prueba física. Dicha aplicación se hace con basamento en el principio de libertad probatoria, el cual no comprende la fenomenología propia de la prueba digital. Bolivia tiene

regulado en el art. 171 del Código de Procedimiento Penal este principio.

Por ejemplo, el art. 174 habla de registro de lugares y de las cosas y el art. 180 y subsiguientes, el allanamiento de domicilio. Ambas disposiciones están redactadas con foco en el sustrato material de lo registrado o allanado. El art. 184 regula la entrega de objetos, instrumentos y demás piezas de convicción existentes, con foco también en la materialidad de las cosas. Dicho artículo regula además la orden de presentación, de la misma manera, así como el art. 218 el pedido de informes.

El art. 186 establece que, si los objetos secuestrados corren riesgo de alterarse, desaparecer, sean de difícil conservación o perecederos, se ordenarán reproducciones, copias o certificaciones sobre su estado y serán devueltos a sus propietarios. Esta disposición tampoco brinda soluciones adicionales respecto al registro del dispositivo antes o después de la posible realización de dicha copia.

Respecto del secuestro de correspondencia, el art. 190 habla de correspondencia, documentos y papeles privados o públicos.

Por último, el capítulo de pericias, el cual muchas veces se utiliza para fundar la apertura y registro de dispositivos electrónicos, posee reglas generales de designación de peritos, el informe, excusa y recusación, aplicables a todos los tipos de pericias, sin especificar nada sobre prueba electrónica.

Por ende, Bolivia, debe trabajar en una reforma de su ley procesal a fin de incorporar medidas relativas a la prueba electrónica. También podría fomentar la adhesión al Convenio de Budapest.

Brasil

Brasil no es parte del Convenio de Budapest, aunque ha iniciado el proceso para la adhesión y es país invitado. En su Código de Proceso Penal no posee normativa específica aplicable en materia de prueba digital.

No obstante, Brasil sancionó una Ley de Marco Civil de Internet (Ley 12965 del 2014, reformada en 2018), donde se reconocen el respeto de ciertos derechos de los usuarios como la intimidad, neutralidad de la red, libertad de expresión, protección de datos personales, estabilidad y funcionalidad, etc.

En esa Ley, Brasil regula algunas disposiciones aplicables en materia de prueba digital. Por ejemplo, el art. 10.1 dice que el prestador responsable de la custodia solo estará obligado a poner a disposición los registros de conexión y acceso a las aplicaciones de Internet, de forma autónoma o asociada a datos personales u otra información que pueda contribuir a la identificación del usuario o del terminal, solamente mediante orden judicial. Lo mismo respecto del contenido de las comunicaciones privadas.

El art. 13 establece la mencionada obligación de retención por el período de un año. En este sentido, el instituto de aseguramiento, en tanto medida cautelar en un proceso penal concreto, pierde relevancia dado que hay una obligación general de retener estos registros de todos los usuarios. Al menos para este tipo de datos (registros de conexión). El art. 5.6 dice que estos registros son la información sobre la fecha y hora de inicio y finalización de una conexión a Internet, su duración y la dirección IP utilizada por el terminal para enviar y recibir paquetes de datos.

Cobrará relevancia la medida de aseguramiento para el resto de los datos informáticos tales como abonado y contenido. En este sentido, el art. 13.2 establece que, la autoridad policial

o administrativa o el Ministerio Público, podrán solicitar cautelarmente que los registros de conexión se conserven por un período superior. Por ende, el primer tramo de conservación de registros de tráfico se regirá por la disposición de retención, y, el tramo extra, por la conservación o aseguramiento de datos regulada en este art. 13.2.

El art. 13.3 agrega que, una vez solicitada la conservación por el plazo adicional al deber de retención, la autoridad tendrá 60 días para acceder a los datos con la autorización judicial correspondiente. Se regula también el deber de confidencialidad. El art. 13.5 vuelve a reforzar lo ya establecido sobre la entrega de información diciendo que la puesta a disposición del solicitante de los registros deberá ir precedida de autorización judicial.

El art. 15 establece la mentada obligación de retención por seis meses para los registros de acceso a las aplicaciones de Internet. Luego se establecen las mismas disposiciones ya comentadas sobre conservación específica por un plazo adicional, y necesidad de orden judicial para el acceso a tales datos.

La orden de presentación se regula en el art. 22 de esta ley. En concreto se establece que el interesado podrá, a los efectos de conformar un conjunto probatorio en un proceso judicial civil o penal, solicitar al juez que ordene al custodio responsable, que proporcione registros de conexión o registros de acceso a las aplicaciones de Internet. No hace referencia propiamente a datos de contenido, sino a tales registros.

También regula que la solicitud deberá contener, bajo pena de inadmisibilidad, prueba fundamentada de la ocurrencia del delito, justificación motivada de la utilidad de los registros solicitados con fines de investigación o instrucción probatoria, y período al que se refieren los registros. Asimismo, corresponderá al juez tomar las medidas necesarias para garantizar la confidencialidad de la información recibida y preservar la intimidad, el honor y la imagen del usuario. Como puede evidenciarse, son normas pensadas y adaptadas para la prueba digital.

Sobre el contenido de la comunicación, el art. 10.2 dice que, el contenido de las comunicaciones privadas solo podrá ser puesto a disposición por orden judicial, en los casos y en la forma que establezca la ley, sin brindar precisiones adicionales.

Brasil tiene en su Ley de intervención de comunicaciones del año 1996 la facultad de la interceptación de comunicaciones telefónicas, de cualquier naturaleza, sin brindar mayores precisiones en cuanto a su objeto, en parte por la tecnología existente en el año de su sanción. Esta ley fue modificada en 2019 y se agregó la posibilidad de realizar la captura ambiental de señales electromagnéticas, ópticas o acústicas cuando la prueba no puede realizarse por otros medios disponibles e igualmente eficaces, y existan elementos probatorios razonables de autoría y participación en infracciones penales cuyas penas máximas sean superiores a 4 (cuatro) años o en infracciones penales conexas. La aplicación debe describir en detalle el lugar y la forma de instalación del dispositivo de captura ambiental. Se debe describir, en detalle, el lugar y la forma de instalación del dispositivo de captura ambiental. El plazo máximo será 15 días prorrogables.

En conclusión, Brasil tiene algunas disposiciones aplicables a la prueba digital, aunque sería oportuno que Brasil concluya su trámite de adhesión al Convenio de Budapest y complete el catálogo de medios de prueba previstos de manera especial para la prueba digital.

Chile

En el Código Procesal Penal de Chile dictado en 2000 y actualizado hasta 2020 se regulan medidas de investigación relacionadas con prueba física. Esto quiere decir que no hay disposiciones específicas que tengan relación con la prueba digital, las cuales serán aplicadas con base al principio de libertad probatoria regulado en el art. 295.

El art. 188 refiere de manera genérica que los objetos, documentos e instrumentos de cualquier clase que parecieren haber servido o haber estado destinados a la comisión del hecho investigado, o los que de él provinieren, o los que pudieren servir como medios de prueba, así como los que se encontraren en el sitio del suceso, serán recogidos, identificados y conservados bajo sello. La alocución de cualquier clase servirá para incluir allí los datos electrónicos contenidos en dispositivos y medios de almacenamiento digital. No obstante, no se regula ninguna disposición especial que haga frente a la realidad de la prueba digital como la manera de proceder a esa recolección, su preservación y aseguramiento de cadena de custodia, ni mucho menos cómo registrarlos.

El art. 205 referido a la entrada y registro está pensado exclusivamente para lugares cerrados como edificio s o lugares cerrados como receptáculos de personas (y no de datos informáticos), dado que dice expresamente: cuando se presumiere que el imputado, o medios de comprobación del hecho que se investigare, se encontrare en un determinado edificio o lugar cerrado, se podrá entrar al mismo y proceder al registro.

Lo mismo sucede con el art. 217 que habla de la incautación de objetos y documentos relacionados con el hecho investigado y que sirvieran de medio de prueba. Esta norma refiere a la materialidad física. En el caso de la prueba digital podría ser aplicable al soporte donde se alojan los datos en tanto sustrato físico. No obstante, no hay disposiciones específicas relativos al registro y secuestro de los datos propiamente dichos, tal como propone por ej. el art. 19 del Convenio de Budapest.

Por su parte, el art. 218 relativo a retención de correspondencia, si bien refiere a correspondencia postal, telegráfica o de otra clase y por ende podría interpretarse que se aplica a lo electrónico, las disposiciones que regula refieren también a la evidencia física no receptando los desafíos de la prueba digital. El art. 219 establece que el juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas.

Respecto a la intervención de comunicaciones el art. 222 habla de la interceptación y grabación de las comunicaciones telefónicas o de otras formas de telecomunicación del sospechado, debiendo indicar en la orden plazo y modo de hacerlo. Además, crea el deber para las empresas de telefonía y comunicaciones de colaborar. Esta norma agrega que los proveedores deberán tener a disposición del Ministerio Público un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. Por lo cual ordena registrar los datos de abonado de los clientes.

El capítulo de prueba pericial, que generalmente en muchos países se utiliza para fundar un registro de dispositivos electrónicos, no refiere a la prueba electrónica, sino que regula aspectos generales como designación del perito, el informe, costas, etc.

En Chile se presentó un proyecto de ley que adecúa la normativa al Convenio de Budapest, (Boletín N.º 12.192-25), el cual regula mayormente delitos relacionados a la tecnología.

Por ende, sería propicio en Chile incorpore medidas procesales relacionadas con prueba digital de manera expresa que hagan realidad a este nuevo paradigma, teniendo en cuenta,

además, que Chile es parte del Convenio de Budapest desde el año 2017. En 2018 se presentó bajo número de Boletín 12192-25 un proyecto de Ley denominado Proyecto que establece normas sobre delitos informáticos, deroga la ley N.° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. Este proyecto, además de regular delitos informáticos, establece disposiciones específicas sobre prueba digital como la preservación rápida de datos, orden de presentación, intervención de las comunicaciones y conservación de los datos relativos al tráfico, entre otras medidas.

Colombia

Colombia es parte del Convenio de Budapest desde el año 2020. Si bien sancionó una ley de delitos informáticos en 2009, no sucedió lo mismo con las medidas de prueba digital. En el Código de Procedimiento Penal de Colombia no se regulan disposiciones específicas.

El art. 213 establece que inmediatamente se tenga conocimiento de la comisión de un hecho que pueda constituir un delito, el servidor de Policía Judicial se trasladará al lugar de los hechos y lo examinará minuciosa, completa y metódicamente, con el fin de descubrir, identificar, recoger y embalar, de acuerdo con los procedimientos técnicos establecidos en los manuales de criminalística, todos los elementos materiales probatorios y evidencia física que tiendan a demostrar la realidad del hecho y a señalar al autor y partícipes del mismo. La disposición refiere a evidencia física. Según el art. 275 que define qué debe entenderse por evidencia física y elementos materiales probatorios, uno de sus incisos dice que la constituye el mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen.

Respecto al registro y secuestro también se hace mención a la evidencia física en el art. 219: el fiscal encargado de la dirección de la investigación, según lo establecido en los artículos siguientes y con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado, podrá ordenar el registro y allanamiento de un inmueble, nave o aeronave, el cual será realizado por la policía judicial.

No obstante, con una ubicación sistemática que quizás no es la mejor dado que su ubica en el capítulo de la intervención de comunicaciones, en el art. 236 se regula lo siguiente: cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso.

Como puede verse es una especie de medida de registro y secuestro de datos informáticos. Luego se establece en el art. siguiente una audiencia de control de legalidad posterior a la medida.

Con relación a la interceptación de comunicaciones, el Código de Procedimiento Penal de Colombia establece en art. 235 que el fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados,

indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. Posee una amplitud en su objeto suficiente como para abarcar distintos tipos de comunicaciones. Luego se establecen plazos y requisitos de la orden.

El art. 244 regula la búsqueda selectiva en bases de datos mediante las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público. Esto podría referir a técnicas de OSINT, pero no de manera clara o expresa.

También se regula un proceso de búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas. Para ello deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente, las disposiciones relativas a los registros y allanamientos.

Dado que Colombia es parte del convenio de Budapest desde el año 2020, deberá trabajar en adecuaciones para la normativa procesal restante, referida a prueba electrónica.

Costa Rica

Costa Rica ratificó el Convenio de Budapest 22 de septiembre de 2017 y previo a su adhesión a dicho instrumento ya contaba con una legislación penal sustantiva.

En Costa Rica, la interceptación e intervención de comunicaciones privadas para propósitos de investigación de delitos graves se lleva a cabo conforme al Capítulo II (Arts. 9-20) de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley No. 7425) en donde necesariamente se requiere la orden de un juez para llevar a cabo una intervención, la cual podrá autorizarse por un plazo máximo de tres meses prorrogable hasta dos veces como máximo. La intervención podrá solicitarse para el esclarecimiento de delitos graves previstos en el Art. 16 de Ley sobre Delincuencia Organizada (Ley No. 8754) entre ellos la explotación sexual en todas sus manifestaciones, la fabricación o producción de pornografía, sustracciones bancarias vía temática, terrorismo y su financiamiento, delitos de carácter internacional, entre otros. Asimismo, conforme al Art. 20 de la Ley No. 7425, las empresas y las instituciones que brindan servicios de comunicación a nivel nacional están obligadas a conceder, a la autoridad judicial- a través de los jueces competentes-, todas las facilidades materiales y técnicas para que las intervenciones sean efectivas, seguras y confidenciales. Respecto a qué tipo de comunicaciones pueden intervenirse, el art. 9 es amplio previendo expresamente las comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales.

Los supuestos de conservación de datos no se encuentran previstos propiamente en el Código Procesal Penal (Ley No. 7594) sino únicamente en la Ley No. 7425 que en su artículo quinto prevé el inventario, custodia y reproducción de documentos por el Tribunal de Justicia y la obtención de copias y reproducciones cuando los documentos secuestrados corran el riesgo de desaparecer, alterarse o sean de difícil custodia. En lo que concierne a las medidas sobre orden de presentación previstas en el Art. 18 del Convenio de Budapest, se argumenta que son posibles en aplicación de lo dispuesto en los artículos 1, 2, 3, 5 a 13 y 20 de la Ley No. 7425 y los Arts. 14 y 17 de la Ley sobre Delincuencia Organizada (Ley No. 8754), pero de manera muy genérica en base a obtención de copias o reproducciones cuando corran riesgo de desaparecer, alterarse, sean de difícil custodia o así convenga al proceso. Asimismo, dichos artículos regulan atribuciones generales del juez en la investigación pudiendo el registro, el secuestro y el examen de cualquier documento privado, siempre que pueda servir como prueba. Por ende, son normas muy inespecíficas y generales. Respecto

de registro y secuestro de datos informáticos no hay normativa específica.

En el marco del proyecto Glacy del Consejo de Europa, se elaboró con las autoridades de Costa Rica un Proyecto de Ley que no ha recibido aún tratamiento legislativo.

Cuba

El Código de Procedimiento Penal de Cuba (Ley 5), posee bajo el capítulo de técnicas especiales de investigación algunas medidas relacionadas con la prueba electrónica. Por ejemplo, el art. 110.1 permite la vigilancia electrónica para la investigación de hechos delictivos que por su gravedad, connotación u organización lo requieran. Respecto a medidas de registro y secuestro, orden de presentación o aseguramiento de datos, no hay disposiciones específicas relativas a la prueba digital. Estas medidas están pensadas para la prueba física, como por ejemplo los arts. 126, 135 (recolección o secuestro de armas, instrumentos o efectos de cualquier clase que puedan tener relación con el delito y que se hallen en el lugar en que este se cometió, en sus inmediaciones, en poder del acusado o en otra parte), 215 (entrada y registro de lugares el cual refiere exclusivamente a edificios de habitación de residentes cubanos), etc. El art. 147 establece que se ordenará la práctica de pruebas científico-técnicas en los casos en que se considere necesario para la investigación de los hechos, sin brindar mayores especificaciones, plazos, modo de ordenarla y sobre qué objetos o casos procede.

El capítulo de prueba pericial, que en muchos países se utiliza para fundar un registro de dispositivos electrónicos, no refiere a la prueba electrónica, sino que regula aspectos generales como designación del perito, el informe, inhabilidades para ser perito, etc.

Respecto de la retención y apertura de correspondencia, refiere a libros, documentos, correspondencia escrita, telegráfica y cablegráfica. Estas disposiciones también están pensadas para la evidencia física, dado que refiere por ejemplo a que se debe firmar cada una de las hojas que componen la correspondencia y/o documentación.

En conclusión, Cuba deberá afrontar una reforma del procedimiento penal que recete disposiciones específicas sobre prueba electrónica.

Ecuador

Ecuador realizó una importante reforma de su ley procesal penal en el año 2000 introduciendo como cambio fundamental el sistema acusatorio de persecución penal, abandonando el sistema inquisitivo hasta ese momento vigente. De esa forma, se sumó al movimiento regional de reforma del sistema penal que significó un cambio fundamental para toda la región. Este Código procesal del año 2000 fue modificado en innumerables oportunidades hasta la sanción del Código Orgánico Integral del año 2014, texto legal vigente que surge como consecuencia de la modificación de la Constitución de Ecuador en el año 2008. Este nuevo Código deroga el Código Procesal Penal anterior y unifica todas las normas penales vigente en un mismo código integral.

En el Título IV del Código, artículos 459 y posteriores, establece un conjunto de disposiciones para la investigación de delitos, que incluyen principios generales aplicables a la evidencia, la preservación de la cadena de custodia, así como los criterios para evaluarla.

Sin embargo, la mayoría de estas disposiciones y medidas procesales penales están pensadas para la prueba física, no estableciendo en ninguna de sus normas un tratamiento especial para los dispositivos que almacenan datos informáticos ni para los datos informáticos en sí mismos.

El inc. 6 del art. 499 parece asimilar la prueba digital al documento como medio de prueba, sin hacer diferencia entre las diferentes pruebas digitales que es posible hallar en un sistema informático. En concreto se establece que podrá admitirse como medio de prueba todo contenido digital conforme con las normas del código.

La preservación de datos, orden de presentación, registro y secuestro de datos informáticos almacenados, interceptación en tiempo real de datos de tráfico y de contenido, entre otras medidas, no están reguladas de manera expresa con asidero en la prueba electrónica. Nuevamente, se aplican disposiciones análogas en virtud del principio de libertad probatoria regulado en el art. 454 inc. 4. Esta tendencia a intentar solucionar los problemas que plantea la evidencia digital mediante las normas previstas para la prueba física ha demostrado importantes dificultades en el derecho comparado europeo continental y en los países de la región con sistemas procesales de características similares al de Ecuador. Tanto desde una perspectiva de la eficiencia de las investigaciones como para la protección adecuada de las garantías del proceso penal.

En Capítulo segundo se denomina “Actuaciones y Técnicas especiales de Investigación”. A los fines de este reporte resultan de interés el art. 470 que prevé una garantía en relación con la grabación de comunicaciones personales y el art. 472, inc. 2) en cuanto establece que tendrá carácter restringido la información acerca de datos de carácter personal o que provenga de comunicaciones personales.

El art. 475 de “Retención de correspondencia” asimila la correspondencia epistolar a la electrónica estableciendo las condiciones y garantías para su incorporación a un proceso penal.

Por su parte el art. 476 habla de interceptación de comunicaciones y otros datos informáticos, siendo el objeto material lo suficientemente amplio como para abarcar todo tipo de comunicaciones electrónicas. La norma prevé las condiciones y garantías, tiempo de duración de la medida y la necesidad de orden judicial.

El art. 500 establece pautas para la recolección y presentación de prueba digital. En este sentido este art. dice que el análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses. Asimismo, establece recolección de contenido digital en el lugar del hecho en determinados supuestos, así como la aplicabilidad de la cadena de custodia y preservación de cadena de custodia. Esta norma no regula expresamente los requisitos para ordenar el registro y secuestro.

Respecto al aseguramiento de datos informático, no existe norma expresa en la legislación vigente en Ecuador. Con relación a la orden de presentación, el art. 499 podría ser utilizado para ordenar la presentación de datos dado que refiere a la solicitud de informes sobre datos que consten en registros, archivos, incluyendo los informáticos. No obstante, no brinda más detalles sobre cómo hacerlo o el deber que poseen los prestadores de servicios de internet. Por último, de conformidad con el artículo 84 de la Ley Orgánica de Telecomunicaciones, los proveedores de servicios deben proporcionar a las autoridades competentes la información solicitada dentro del debido proceso, para fines relacionados con la investigación de delitos. Asimismo, los proveedores de servicios de telecomunicaciones deben proporcionar la información en las condiciones técnicas y con los protocolos establecidos por el juez en su orden, o el personal técnico, expertos o investigadores designados por dicha autoridad. Se prohíbe hacer público o comunicar a terceros los requisitos judiciales establecidos.

Ecuador no ha adherido al Convenio de Budapest, por lo que trabajar en el desarrollo en materia de prueba electrónica resulta fundamental. La adecuación del título de “PRUEBA” de la legislación vigente en Ecuador requerirá de la incorporación de nuevos medios de

prueba e investigación, en algunos casos modificando artículos de la ley vigente y en otros agregando nuevos artículos u ordenando adecuadamente algunas de las normas dispuestas en capítulos diferentes del ordenamiento vigente en Ecuador.

En el año 2020, en el marco de cooperación del Proyecto Glacy se elaboró un proyecto de reforma legislativa que prevé la incorporación de los medios de prueba previstos en la Convención de Budapest. El proyecto no recibió aún tratamiento legislativo.

El Salvador

El Salvador posee pocas medidas relacionadas con prueba electrónica reguladas en el Decreto Legislativo Número 904 Código Procesal Penal de la República de El Salvador, modificado entre otros por el Decreto 733. Por ejemplo, regula en el art. 201 la posibilidad de que el fiscal ordene al juez que adopte medidas para la obtención, resguardo o almacenamiento de la información, sin perjuicio que se ordene el secuestro respectivo, sin mencionar su registro o cómo procederse respecto de él.

Asimismo, posee en los art. 250 a 252 tres disposiciones sobre la cadena de custodia. Dichas medidas son limitadas y no reflejan las medidas del convenio.

El resto de las medidas están pensadas para la prueba física, como es por ejemplo el art. 193 de dicho decreto que regula el registro de la morada. Asimismo, el art. 197 regula el registro de otros elementos cuya referencia lo es también a su materialidad física como vehículos, muebles y compartimientos cerrados.

El Salvador no es parte del Convenio de Budapest, por lo que sería oportuno que impulse la adhesión al mismo, así como incorporar medidas procesales sobre prueba digital específicas. Esto porque, si bien El Salvador dio un paso importante sancionando una Ley Especial contra Delitos Informáticos y Conexos, no fue acompañado por una ley similar desde el punto de vista del derecho procesal penal.

Guatemala

Guatemala no posee una legislación sobre medidas procesales, pero en febrero de 2017 elaboró un proyecto de Ley sobre Ciberdelito con el apoyo del Consejo de Europa, con número de registro 5254.

Asimismo, en 2019 se presentó, sobre la base de aquel proyecto, la iniciativa de Ley de Prevención y Protección contra la Ciberdelincuencia con registro 5601. Esta regula los delitos relacionados con la tecnología, y medidas procesales relacionadas con la prueba digital. Los arts. 26 y subsiguientes establecen el aseguramiento de datos informáticos, la orden de presentación, el registro y secuestro de medios digitales o electrónicos, interceptaciones de datos, y cooperación en materia penal y procesal penal. Esta ley tuvo dictamen favorable con modificaciones en fecha 18 de noviembre de 2019 y aún no fue sancionada.

El Decreto número 51-92, Código Procesal Penal de la República de Guatemala, no regula medidas de prueba relacionadas con prueba digital. Todas las disposiciones del Código Procesal Penal giran en torno a la prueba física, y, de pretender su aplicación a la prueba electrónica, el único sustento normativo es el principio de libertad probatoria regulado en el art. 182. Respecto a la intervención de comunicaciones, el art. 205 hace referencia a las comunicaciones telefónicas o “similares”, no hablando de datos de tráfico o contenido.

Guatemala ha demostrado interés en adherir al Convenio de Budapest mediante carta enviada al secretario del Convenio (Alexander Seger - Consejo de Europa) en fecha abril

2016. Luego del procedimiento que establece el propio Convenio sobre el procedimiento de invitación, el 22 de abril de 2020 se envió la invitación formal a Guatemala, la cual expirará en el año 2025.

Honduras

Honduras no posee medidas relacionadas con evidencia digital reguladas en el Decreto 9-99-E Código Procesal Penal de la República de Honduras, ni tampoco es miembro de Convenio para la Ciberdelincuencia de Budapest.

Todas las medidas procesales del Código giran en torno a la materialidad física de la prueba sin poseer medidas especiales relacionadas con prueba digital. Solamente el art. 216 dice que, para asegurar la eficacia y la calidad de los registros e inspecciones, quienes los practiquen podrán ordenar operaciones técnicas o científicas, y que la participación de testigos, peritos o intérpretes estará sujeta a las reglas establecidas en el código, sin brindar detalles o precisiones adicionales.

Asimismo, el art. 220 sobre reglas que deben aplicarse a las cosas secuestradas, dice que si los objetos secuestrados corren peligro de alterarse o de desaparecer o si son de difícil custodia, se sacarán reproducciones o copias o se certificará su existencia y estado. No hace referencia a computadoras o dispositivos electrónicos de manera expresa, pero se puede utilizar en base al principio de libertad probatoria regulado en el art. 199 para las operaciones de extracción o copias forenses. El mentado artículo dice que los hechos y circunstancias relacionados con el delito objeto del proceso, podrán ser demostrados utilizando cualquier medio probatorio, aunque no esté expresamente regulado en el código, siempre que sean objetivamente confiables. En lo no previsto en el código se estará a lo dispuesto en las normas que regulen el medio de prueba que más se asemeje.

La Ley Especial sobre Intervención de las Comunicaciones Privadas (Decreto 243-2011) derogó el artículo 223 del Código Procesal Penal de Honduras que regulaba la intervención de las comunicaciones. Este artículo decía que el juez, a petición del Ministerio Público, podía ordenar, mediante resolución fundada, la grabación de las comunicaciones telefónicas, informáticas o de cualquier otra índole. El Decreto 243-2011 regula la intervención de las comunicaciones de cualquier tipo, no refiriendo únicamente a las telefónicas. Así figuran los principios, el procedimiento, los requisitos, la competencia, el contenido de la solicitud, entre otros supuestos. Por ejemplo, en el artículo 30, se establece que aquellas comunicaciones que se encuentran cifradas o codificadas, o protegido por contraseña, el Juez de Garantía ordenará las diligencias necesarias para acceder a su contenido.

Es conveniente que Honduras incorpore medios de prueba que refieran expresamente a lo electrónico, así como la adhesión a un instrumento internacional como lo es el convenio de Budapest.

México

Con respecto a medidas de carácter procesal en materia de investigaciones sobre ciberdelito, el Art. 381 del Código Nacional de Procedimientos Penales de México reconoce los datos y la información contenida en medios digitales, electrónicos, ópticos o cualquier otra tecnología como medios de admisión de prueba en tribunales en materia penal. Asimismo, cuando no se cuente con los medios necesarios para su reproducción, la parte que los ofrezca los deberá proporcionar o facilitar.

En lo que refiere a intervención de comunicaciones, el art. 291 establece quién y cómo pueden solicitar dicha medida. Respecto al objeto, aplica a todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real. Por ende, el objeto es amplio, pudiendo intervenir cualquier comunicación tecnológica.

Asimismo, dicho artículo regula la extracción de información de dispositivos electrónicos. En este sentido, dicha extracción consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con estos. Su ubicación sistemática no es la mejor, dado que este supuesto estaría refiriendo a un registro y secuestro de datos que incluso no sean comunicaciones, sino cualquier tipo de datos, tal como dice el supuesto con la alocución y todo aquello que pueda contener información. Se regulan plazos y requisitos de la solicitud. El art. 294 vuelve a repetir que podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

La Ley Federal de Telecomunicaciones y Radiodifusión y el código contienen obligaciones para los proveedores de servicios de telefonía móvil para la conservación de datos e información de comunicaciones móviles para propósitos de investigaciones penales, en situaciones de emergencia o cuando esté en peligro la vida de una persona, sin embargo, no resulta claro que dichas disposiciones apliquen directamente a los proveedores de servicios globales de internet. Asimismo, el CNPP carece de los procedimientos, mecanismos y plazos necesarios para ordenar la preservación, producción y secuestro de datos informáticos (datos de abonado y tráfico).

La primera parte del art. 303 del código establece que cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. La Suprema Corte de Justicia invalidó en marzo de 2018 este primer párrafo, por entender que era extremadamente

amplia y sin límites en relación con en la investigación de qué tipos delitos resulta aplicable, plazos, proporcionalidad y otros principios, por lo que deberá reverse.

No hay disposiciones específicas que resulten aplicables a la orden de presentación, a la conservación de datos, o al registro y secuestro, por fuera de lo aquí mencionado. La mayoría de las medidas procesales del código están pensadas para la prueba física. Por lo tanto, sería necesario una reforma, así como adherir al Convenio para la Ciberdelincuencia Budapest.

Nicaragua

En lo que respecta a las medidas procesales sobre prueba electrónica en Nicaragua, en la Ley 406 (Código Procesal Penal aprobado en 2001), solamente hay una disposición que puede referir a esta materia: los arts. 213 y 214. El art. 213 regula la intervención de comunicaciones telefónicas u “de otras formas de telecomunicaciones” en delitos graves.

El art. 214, por su parte, regula la intervención de comunicaciones escritas, telegráficas y electrónicas para los mismos delitos graves del art. 213. La diferencia entre ambos supuestos radica en que el primer artículo refiere a telecomunicaciones, sean telefónicas o de otro tipo pero siempre con los requisitos de una telecomunicación, mientras que el segundo artículo regula con una amplitud mayor cualquier tipo de comunicación (escritas, telegráficas y electrónicas).

Este art. 214 podría ser asimilable a interceptación de datos de contenido, aunque sin ningún límite ni criterio similar al Convenio. El resto de las disposiciones están pensadas para la prueba física, como la disposición de secuestro o de presentación. Por ej. el art. 215 relativo a la orden de secuestro menciona de manera genérica que podrá disponerse la obtención de copias o reproducciones de los objetos secuestrados cuando estos puedan desaparecer o alterarse, sean de difícil custodia o cuando convenga así para la investigación. Si bien puede aplicarse a los dispositivos tecnológicos secuestrados, lo es en base al principio de libertad probatoria únicamente (regulado en art. 15), no previendo supuestos especiales para este tipo de prueba.

La Ley prevención, investigación y persecución del crimen organizado y de la Administración de los bienes incautados, decomisados y abandonados, Ley N° 735 del año 2010, regula en el art. 62 la interceptación de comunicaciones. Esta disposición permite impedir, interrumpir, interceptar o grabar comunicaciones, correspondencia electrónica; otros medios radioeléctricos e informáticos de comunicaciones, fijas, móviles, inalámbricas y digitales o de cualquier otra naturaleza, únicamente a los fines de investigación penal y de acuerdo con las normas establecidas en el Código Procesal Penal. Asimismo genera la obligación a las empresas privadas o públicas prestadoras de los servicios de comunicación telefónica, informática o de otra naturaleza electrónica y otras que utilicen el espectro electromagnético y radioelectrónico, a prestar todas las condiciones y facilidades materiales y técnicas necesarias para que las intervenciones sean efectivas, seguras y confidenciales y estarán obligadas a permitir que se usen sus equipos e instalaciones para la práctica de las diligencias de investigación antes previstas.

Salvo estas aisladas excepciones, Nicaragua no cuenta ni con leyes especiales ni con disposiciones dentro del Código Procesal Penal que hagan frente a la realidad de la prueba electrónica. Dado que tampoco es parte del Convenio de Budapest, Nicaragua deberá trabajar en modificaciones legislativas.

Panamá

Panamá es miembro del Convenio para la Ciberdelincuencia de Budapest desde el año 2014. Además, posee algunas disposiciones relacionadas con la prueba electrónica.

En el Código Judicial, Libro Tercero, referido al procedimiento penal, hay algunas medidas procesales pensadas para la evidencia física que se aplican a la digital. Por ejemplo, el art. 2178 que habla de registro y secuestro dice o cualesquiera otros objetos que puedan servir para comprobar el hecho punible o para descubrir a sus autores y partícipes. Frase utilizada para incluir evidencia digital. El resto de las disposiciones están ideadas para ser aplicadas a la evidencia en soporte físico.

Por su parte, la Ley 121 del 2013 relativa a medidas contra las actividades relacionadas con el delito de delincuencia organizada regula la interceptación de las comunicaciones por cualquier medio tecnológico y la incautación de datos.

Lo mismo respecto del art. 311 del Código Procesal de Panamá (Libro Tercero relativo al procedimiento de investigación) que regula las interceptaciones de comunicaciones. Dicho art. habla de comunicaciones cibernéticas, seguimientos satelitales, vigilancia electrónica y comunicaciones telefónicas, pudiéndose interpretar que alude a interceptación de datos de contenido.

El art. 314 dice regula la incautación de datos. En este sentido menciona que, el examen de equipos informáticos o datos almacenados en cualquier otro soporte se hará bajo responsabilidad del fiscal, citando al imputado y su defensor. Asimismo, el equipo o la información que no resulten útiles a la investigación o comprendidos como objetos no incautables serán devueltos de inmediato y no podrán utilizarse para la investigación.

El art. 304 habla de que el fiscal podrá solicitar en el marco de un allanamiento uno o más peritos para que, bajo su dirección, concurran como auxiliares para el mejor esclarecimiento de los hechos. Esta normativa podría aplicarse en los casos de que se halle evidencia electrónica y sea necesario conocimientos técnicos. No obstante, la norma está regulada de una manera amplia y general, no aludiendo específicamente a este supuesto.

Respecto del aseguramiento de datos informáticos, el art. 383 del Código Procesal de Panamá dice que podrán tomarse las medidas necesarias para evitar que los elementos materiales de prueba sean alterados, ocultados o destruidos. Para esa finalidad, previa solicitud de parte interesada, el Juez de Garantías o los tribunales podrán ordenar las que estimen necesarias, ajustándose a los principios o reglas del debido proceso. Es una norma amplia que, si bien no menciona plazos ni mecanismos, puede ser usada para fundar dicha medida, en base al principio de libertad probatoria regulado en el art. 376.

Panamá trabajó en un Proyecto de Ley con asistencia de expertos del Consejo de Europa, bajo número 558, que modifica y adiciona artículos al Código Penal, relacionados al Cibercrimen. En él, además de modificarse delitos relacionados con la tecnología añadiéndolos Código Penal, se incorpora en medidas relacionadas con prueba electrónica modificando el artículo 338 del Código Procesal Penal. En este sentido planea agregar los incisos A a F, legislando la conservación de datos informáticos, orden de presentación, accesos transfronterizos de datos abiertos, obtención en tiempo real de datos de tráfico y de contenido.

A fin de lograr una mayor adecuación al Convenio de Budapest, es necesario que Panamá logre la sanción del mencionado Proyecto de Ley número 558.

Paraguay

El Código Procesal Penal de Paraguay (Ley No. 1286/1998), carece de una regulación específica en relación con los medios de prueba digital. Por este motivo, actualmente los operadores del sistema penal aplican por analogía para la incorporación al proceso de pruebas electrónicas los medios de prueba que regulan la prueba física, en base al principio de libertad probatoria regulado en el art. 173.

En Paraguay, la interceptación y el secuestro de la correspondencia se lleva a cabo conforme al Art. 198 del Código Procesal Penal en donde necesariamente se requiere la orden de un juez para llevar a cabo una intervención. Sin embargo, dicha disposición no establece un plazo máximo ni la posibilidad de prorrogar la medida.

No se regula la conservación rápida de datos informáticos almacenados. La Ley No. 4868 de Comercio Electrónico, no da respuesta concreta para esta medida.

En lo que concierne a las medidas sobre orden de presentación tampoco se encuentra prevista en el Código Procesal Penal de Paraguay de manera expresa para los datos informáticos. En la práctica se aplican las normas procesales tradicionales sobre pedidos de informes y la orden de presentación de elementos físicos.

Con respecto a las medidas sobre registro y secuestro de datos informáticos almacenados, al no existir una norma expresa, se utiliza por analogía lo dispuesto en los artículos 183, 192, 193, 196 y 198 del Código Procesal Penal donde se regulan con carácter general las medidas de investigación y registro de lugares públicos, orden de operaciones técnicas o científicas, reconocimientos y reconstrucciones y cuestiones relacionadas a la intercepción y secuestro de correspondencia.

El Art. 200 faculta a los jueces poder ordenar la intervención de las comunicaciones del imputado a través de cualquier medio técnico. Asimismo, el Art. 198 que permite la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase. Estas medidas no están directamente relacionadas con las facultades de interceptación de datos de contenido y de tráfico. Si bien refiere el art. 200 a comunicaciones cualquiera sea el medio técnico utilizado para conocerlas, por lo que podría aplicarse a datos de tráfico y contenido de comunicaciones digitales, no regula el detalle necesario que requiere la intervención de este tipo de datos, así como el deber de colaboración de los proveedores de internet.

Por ende, Paraguay debe reformar su Código Procesal a fin de incorporar medios de prueba especiales para la prueba digital, para profundizar la implementación del Convenio de Budapest, al cual adhirió en 2018.

En el año 2020, en el marco del proyecto Glacy se elaboró un proyecto de ley que preveía la incorporación de los medios de prueba y las normas de cooperación internacional previstos en la convención de Budapest. El proyecto no fue tratado aún.

Perú

Perú posee diversas leyes que regulan la materia investigativa relacionada con prueba digital: el Código Procesal Penal, la Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional 27697, la Ley de Delitos Informáticos 30096, Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, y la Ley contra el Crimen Organizado 30077.

La Ley de Delitos Informáticos modifica el art. 230.4 del Código Procesal Penal regulando la intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación. En concreto permite que las empresas de servicios públicos de telecomunicaciones faciliten, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. De esta manera se regula la intervención en tiempo real de datos de contenido y de tráfico, conforme los artículos 20 y 21 del Convenio de Budapest.

La Ley de Delitos Informáticos modifica la Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, para que también sean aplicadas en la persecución de delitos informáticos (no menciona delitos en general que posean evidencia digital, sino literalmente delitos informáticos regulados en la ley de delitos informáticos).

Respecto a esta Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional regula para determinados delitos (agregando los delitos informáticos), la posibilidad de conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional. La ley regula con detalle quién puede solicitarlo, con qué requisitos y cómo se procederá. El art. 4 tiene una disposición general de extensión de la cobertura de esta ley a otros documentos privados, diciendo que se aplicará también para los libros, comprobantes y documentos contables y administrativos, así como todo otro documento privado que pueda ser útil para la investigación.

Respecto al Código Procesal Penal de Perú, regula en el art. 157 el principio de libertad probatoria, sobre el que se aplicarán mucha de las disposiciones procesales previstas. No hay disposiciones específicas sobre prueba digital. Por ejemplo, los arts. 184 y 188 que regulan la orden de presentación, refiere a todo documento que puede servir como medio de prueba. Lo mismo sucede con las disposiciones relativas al allanamiento y al registro y secuestro de cosas. En este sentido el artículo 233, por ejemplo, menciona que se podrá incautar documentos privados útiles para la investigación, cuando existan motivos suficientes para estimar que una persona tiene en su poder. El código no brinda detalles adicionales sobre qué debe entenderse por documentos privados.

En el artículo 207 y subsiguientes, se regula la videovigilancia en investigaciones por delitos violentos, graves o contra organizaciones delictivas. Esto procede para realizar tomas fotográficas y registro de imágenes, utilizar otros medios técnicos especiales determinados con finalidades de observación o para la investigación del lugar de residencia investigado.
Perú es miembro del Convenio de Budapest desde el año 2018. Más allá de las disposiciones detalladas, Perú deberá trabajar en una modificación de su normativa procesal, a fin de incorporar los medios de prueba faltantes.

Uruguay

Uruguay no es parte del Convenio de Budapest. En su Código de Proceso Penal no posee normativa específica aplicable en materia de prueba digital.

Posee normas generales dirigidas a la actuación de las fuerzas del orden de Uruguay en el art. 53, donde se prevé por ejemplo el resguardo, evitar la alteración o borrado de cualquier forma de los vestigios del hecho, etc. Esta medida, si bien no refiere específicamente a la orden de conservación de datos informáticos, por la aplicación del principio libertad probatoria podría utilizarse para fundar una orden de conservación. No obstante, es una medida que no recepta de manera expresa, ni hace alusión a las características de aquella. El principio de libertad probatoria, en Uruguay, está previsto en el art.144 del Código.

El resto de las medidas procesales del Código de Proceso Penal de Uruguay tampoco refieren a la prueba digital. Por ejemplo, el art. 173 regula la orden de presentación, la cual hace referencia a todo documento que pueda servir como medio de prueba. Quien lo tenga en su poder, estará obligado a presentarlo, exhibirlo o permitir su conocimiento, pero no hace alusión a datos informáticos, o datos tales como datos de contenido, de abonado, o de tráfico. Por su parte, el art. 177 refiere al requerimiento de informes sobre datos que constan en registros oficiales o privados. Esta medida tampoco hace referencia a la prueba digital.

Respecto al registro y secuestro de datos informáticos tampoco hay una medida específica aplicable. El Código de Proceso Penal de Uruguay prevé un capítulo general de prueba pericial, con las críticas que ya hemos realizado en este informe sobre recurrir a tal medida para realizar un registro y secuestro de datos informáticos, dado que no regula ningún supuesto específico aplicable a la prueba electrónica.

El resto de las medidas hacen alusión a la prueba física, tal como sucede en la mayoría de los códigos de la región, hablando de lugares. La norma de exhibición e incautación de bienes del art. 197 lo mismo, al hablar de exhibir un bien, lo que difícilmente capta el paradigma del dato informático y la prueba digital. A lo sumo esta medida podrá aplicarse para el secuestro del soporte, pero esta acción no habilita el ingreso al contenido del dispositivo. Por su parte el art. 199 habla de que los bienes objeto de secuestro o incautación serán registrados y debidamente individualizados, haciendo referencia a la materialidad del objeto.

Por su parte el art. 203 regula la posibilidad de incautar los documentos públicos y privados, lo que tampoco recepta la prueba digital ni regula mecanismos específicos.

La única disposición aplicable a la prueba digital es el art. 205 del código. Esta dice que el Ministerio Público solicitará al tribunal competente la interceptación, incautación y ulterior apertura o registro de cualquier correspondencia, envío postal, correo electrónico o similar (…). Si bien esta medida dice, además de correo electrónico, o similar, no puede pretenderse que sea un cajón de sastre donde pueda ingresar así sin más todo tipo de tecnología, tal como ya hemos comentado sobre este tipo de expresiones.

Lo mismo sucede con la norma de intervención grabación o registro de comunicaciones telefónicas u otras formas de comunicación del art. 208. La misma dice que el fiscal podrá solicitar al juez la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Mas allá que esta disposición trae garantías adicionales como lo que debe contener la orden judicial y plazo, resulta aplicable los comentarios sobre las expresiones generales como u otras formas de comunicación, que utiliza este artículo.

Por último, el art. 210 regula la video vigilancia sin conocimiento del afectado, en lugares abiertos expuestos al público. Cuando se realice en interior de inmuebles o lugares cerrados se requerirá orden judicial.

En conclusión, Uruguay deberá realizar una reforma a su Código Procesal a fin de hacer frente al paradigma de la prueba digital receptando disposiciones específicas, así como analizar la posibilidad de adherir a un instrumento internacional como el Convenio de Budapest.

Segunda parte: técnicas especiales de investigación tecnológica

Frente a nuevos desafíos que plantea el avance de la tecnología y su uso tanto para comisión de delitos informáticos como para el resguardo de información que puede ser relevante para la investigación de cualquier delito (a modo de ejemplo, la encriptación, el anonimato en la navegación, el alojamiento de información en la nube, etc.) que torna más dificultosa la investigación por parte de los estados, ha surgido la necesidad de nuevos medios de investigación tecnológica que requieren una adecuada regulación que prevea un balance adecuado entre la necesidad estatal de persecución penal y protección de las víctimas con la protección de las garantías del proceso penal y la protección de datos personales.

En este sentido, la realización de operaciones encubiertas en el ciberespacio, entregas vigiladas de contenido ilegal en red, el uso de programas maliciosos por parte del estado, el uso de drones, etc., constituyen nuevos desafíos para la normativa procesal penal.

Son pocos los países que tienen legisladas estos tipos de medidas especiales de investigación de manera especial atendiendo a las características de las investigaciones en entornos digitales.

A continuación, analizaremos qué países poseen en sus legislaciones técnicas especiales de investigación en entornos digitales como agente encubierto digital y/o entregas vigiladas.

Los países no mencionados en el análisis poseen la figura de agente encubierto o entregas vigiladas tradicionales sin disposiciones especiales aplicables a la evidencia digital, tal como Bolivia, Chile, Ecuador, El Salvador, México, Nicaragua y Uruguay.

Argentina

Argentina posee en el ya mencionado Código Procesal Penal Federal, el cual se encuentra actualmente en implementación, un capítulo denominado técnicas especiales de investigación. Están diseñadas para ser aplicadas a determinados delitos como por ejemplo los relacionados con estupefacientes, aduaneros, delitos agravados por finalidades terroristas, secuestro de personas, trata de personas, asociaciones ilícitas, delitos contra el orden económico. Entre las medidas especiales se regula el agente encubierto, el cual es aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que prestando su consentimiento y ocultando su identidad, se infiltre o introduzca en las organizaciones criminales o asociaciones delictivas, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial, conforme el art. 175 ter. Su actuación es dispuesta por el juez a pedido del Ministerio Público Fiscal.

También prevé el agente revelador, informantes y acuerdos de colaboración.

Respecto a las entregas vigiladas el art. 175 terdecies establece que el juez, a pedido del representante del Ministerio Público Fiscal, podrá autorizar que se postergue la detención de personas o el secuestro de bienes cuando estime que la ejecución inmediata de dichas medidas puede comprometer el éxito de la investigación preparatoria. También podrá, incluso suspender la interceptación en territorio argentino de una remesa ilícita y permitir que entren, circulen o salgan del territorio nacional, sin interferencia de la autoridad competente y bajo su control y vigilancia, con el fin de identificar a los partícipes, reunir información y elementos de convicción necesarios para la investigación, siempre y cuando se tuviere la seguridad de que será vigilada por las autoridades judiciales del país de destino.

Cabe señalar que estas disposiciones no refieren expresamente a su realización mediante medios informáticos como hace por ejemplo la legislación española. No obstante, dada la amplitud del término infiltre o introduzca en las organizaciones criminales o asociaciones delictivas, puede abarcar múltiples modalidades. Lo mismo con las entregas vigiladas y las remesas indebidas.

Respecto a la ley 27319, Argentina sancionó como ley independiente al Código Procesal Penal las medidas de Investigación, Prevención y Lucha de los delitos complejos. Esto significa que no hace falta esperar a que se implemente el Código Procesal Penal Federal para su uso.

Las medidas no varían en su redacción, pero sí respecto a los delitos aplicables. Esta ley agrega que puede aplicarse a la investigación de material de explotación sexual infantil, prostitución infantil y corrupción de menores de edad. Por lo que, si bien de manera expresa el agente encubierto o entregas vigiladas no refieren a operaciones en la red, dado que pueden aplicarse al delito de material de explotación sexual infantil, podría ser utilizado para realizar investigaciones encubiertas o entregas vigiladas de ese material en la red, sea superficial o profunda.

No obstante, sería ideal se reforme la ley a fin de incorporarlo a otros tipos de delitos que pueden requerir el uso de estas técnicas como el grooming, daños informáticos, etc. Asimismo, podría regularse expresamente la modalidad informática a fin de regular pormenores del mundo digital como qué sucedería en caso de que se obtengan pruebas en extraña jurisdicción durante su ejecución, o deba ejercer actos lesivos de derechos al realizar la maniobra.

La Provincia de Corrientes, por ejemplo, regula la vigilancia remota sobre equipos informáticos estableciendo que podrá autorizarse el acceso remoto al contenido de ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos, a través de un software que lo permita o facilite. El juez podrá exigir al fiscal que precise la forma en que se procederá al acceso y captación de los datos o archivos informáticos, así como la identificación del software mediante el cual se ejecutará el control de la información. También establece otros tipos de vigilancias como la acústica, de imagen, etc., en un capítulo específico denominado “medidas especiales de investigación”.

Brasil

La Ley 13964 de Mejora la Legislación Penal y el Procedimiento Penal de 2019, modifica la Ley 12850 de Organizaciones e Investigación Criminales, regula la posibilidad de utilizar agente encubierto digital para investigar organizaciones criminales, así como otras medidas especiales.

Respecto a los delitos aplicables, son aquellos cometidos por organizaciones delictivas, definiendo a tales como la asociación de cuatro o más personas ordenadas estructuralmente y caracterizadas por la división de tareas, aunque informal, con el objetivo de obtener, directa o indirectamente, una ventaja de cualquier naturaleza, mediante la práctica de infracciones penales cuyas penas máximas sean superiores a cuatro años, o que sean de carácter trasnacional. También se aplica la ley a las infracciones penales previstas en un tratado o convención internacional cuando, una vez iniciada la ejecución en el país, el resultado haya o debió haber ocurrido en el extranjero, o viceversa, y delitos de organizaciones terroristas, entendidas como aquellas destinadas a la práctica de actos de terrorismo legalmente definidos.

El art. 10 de la Ley 12850 reformada por Ley 13964, establece la posibilidad de infiltrar policías en labores de investigación, solicitados por el Ministerio Público, previa manifestación técnica del jefe policial cuando así lo solicite en el curso de la investigación policial, precedida de una minuciosa, motivada y confidencial Autorización del sistema judicial, que establecerá sus límites. Dice que se admitirá la infiltración si existen indicios de infracción penal, o y si la prueba no puede presentarse por otros medios disponibles. Se regulan plazos máximos de seis meses con posibles renovaciones, los informes a presentar, etc.

Hasta aquí, la medida no difiere en los sustancial a lo regulado por Argentina. No obstante Brasil regula expresamente la modalidad virtual del agente encubierto en el art. 10A.

En concreto establece que se admitirá la actuación de policías virtuales infiltrados, cumpliendo con los requisitos del artículo anterior, en internet, con la finalidad de investigar los delitos previstos en la Ley de Organizaciones e Investigación Criminales, practicados por organizaciones delictivas, siempre que se demuestre su necesidad y se indique el alcance de las funciones de los policías, los nombres o apellidos de las personas investigadas y, cuando sea posible, los datos de conexión o registro que permitan la identificación de estas personas. La ley dice que por datos de conexión deberá entenderse la información relativa a la hora, fecha, inicio, finalización, duración, dirección de Protocolo de Internet (IP) utilizada y terminal de origen de la conexión, y por datos de registro, la información relativa al nombre y dirección del suscriptor o usuario registrado o autenticado para la conexión a quien se asignó la dirección IP, identificación de usuario o código de acceso en el momento de la conexión. Luego replica los mismos límites, plazos e informes que para el agente encubierto no digital.

El art. 10C agrega la posibilidad de usar un policía que oculta su identidad para, a través de Internet, recabar pruebas de la autoría y materialidad de los delitos, respondiendo de los excesos cometidos durante la misma. El juez deberá analizar todo.

Luego la ley dice que los actos electrónicos registrados serán recogidos en registros separados y adjuntos al proceso penal junto con la investigación policial, asegurando la preservación de la identidad del agente policial infiltrado y la intimidad de los involucrados.

Para la procedencia del agente encubierto tradicional y el digital, conforme el art. 11, la solicitud del Ministerio Público para la infiltración de agentes contendrá la demostración de la necesidad de la medida, el alcance de las funciones de los agentes y, cuando sea posible, los nombres o apellidos de las personas investigadas y la infiltración del lugar.

También se agrega que los órganos públicos de registro podrán incluir en sus propias bases de datos, mediante procedimiento confidencial y con solicitud de la autoridad judicial, la información necesaria para la efectividad de la identidad ficticia creada, en los casos de infiltración de agentes en Internet.
La Ley tiene una cláusula de eximición de responsabilidad penal, diciendo que no es punible, en el ámbito de la infiltración, la práctica delictiva por parte del agente infiltrado en el curso de la investigación, cuando no sea exigible una conducta diferente.

El art. 8 regula las entregas vigiladas, aquí denominadas acciones controladas, consistente en retrasar la intervención policial o administrativa relacionada con la acción realizada por una organización delictiva o relacionada con ella, siempre que se mantenga bajo observación y seguimiento para que la medida judicial se lleve a cabo en el momento más efectivo para la formación de pruebas y la obtención de información. No hay regulaciones especificas en esta medida aplicables a la evidencia electrónica.
También regula la Ley 12850 otras medidas de investigación especiales como la captura ambiental de señales electromagnéticas, ópticas o acústicas, el acceso a registros de llamadas telefónicas y telemáticas, datos de registro contenidos en bases de datos públicas o privadas e información electoral o comercial, interceptación de comunicaciones telefónicas y telemáticas, ya analizadas en la primera parte de este capítulo del informe.

Colombia

En el ya mencionado Código de Procedimiento Penal de Colombia, el art. 242 B incorpora las operaciones encubiertas en medios de comunicación virtual utilizando un agente encubierto.

El art. 241 regula la medida tradicional diciendo que, cuando el fiscal tuviere motivos razonablemente fundados para inferir que el indiciado o el imputado pertenece o está relacionado con alguna organización criminal, ordenará a la policía judicial la realización del análisis de aquella con el fin de conocer su estructura organizativa, la agresividad de sus integrantes y los puntos débiles de la misma. Después, ordenará la planificación, preparación y manejo de una operación, para que agente o agentes encubiertos la infiltren con el fin de obtener información útil a la investigación que se adelanta.

El art. 242 establece específicamente el agente encubierto tradicional con algunos matices previendo la utilización de agentes encubiertos, siempre que resulte indispensable para el éxito de las tareas

investigativas. En desarrollo de esta facultad especial podrá disponerse que uno o varios funcionarios de la policía judicial o, incluso particulares, puedan actuar en esta condición y realizar actos extrapenales con trascendencia jurídica. En consecuencia, dichos agentes estarán facultados para intervenir en el tráfico comercial, asumir obligaciones, ingresar y participar en reuniones en el lugar de trabajo o domicilio del indiciado o imputado y, si fuere necesario, adelantar transacciones con él. Igualmente, si el agente encubierto encuentra que en los lugares donde ha actuado existe información útil para los fines de la investigación, lo hará saber al fiscal para que este disponga el desarrollo de una operación especial, por parte de la policía judicial, con miras a que se recoja la información y los elementos materiales probatorios y evidencia física hallados.

Asimismo, podrá disponerse que actúe como agente encubierto el particular que, sin modificar su identidad, sea de la confianza del indiciado o imputado o la adquiera para los efectos de la búsqueda y obtención de información relevante y de elementos materiales probatorios y evidencia física.
Durante la realización de los procedimientos encubiertos podrán utilizarse los medios técnicos de vigilancia y seguimiento pasivo electrónico de personas.

Para la medida de agente encubierto se establece un plazo máximo de un año prorrogable por otro año más con debida justificación.

Una vez regulada esta medida tradicional con los matices de que puedan serlo personas particulares de confianza del investigado, el art. 242 B regula la modalidad digital.

Bajo el título “operaciones encubiertas en medios de comunicación virtual”, el artículo establece que la técnica especial de investigación de agente encubierto contemplado en el artículo 242, ya analizada, podrá utilizarse cuando se verifique la posible existencia de hechos constitutivos de delitos cometidos por organizaciones criminales que actúan a través de comunicaciones mantenidas en canales cerrados de comunicación virtual.

El agente encubierto podrá intercambiar o enviar archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. También obtener imágenes y grabaciones de las conversaciones que puedan mantenerse en los encuentros previstos entre la gente y el indiciado.

En todo caso, tratándose de este tipo de operaciones encubiertas, se deberá contar con una autorización previa por parte del Juez de Control de Garantías para interferir en las comunicaciones.

Cuba

Cuba posee en su Ley de Procedimiento Penal una única disposición bajo el título de Técnicas Especiales de Investigación, el art. 110.1 que dice que son técnicas especiales de investigación, a los efectos de esta ley, la investigación encubierta, el colaborador eficaz, el empleo de la vigilancia electrónica o de otro tipo y las entregas vigiladas, siempre que resulten idóneas o necesarias para la investigación de hechos delictivos que por su gravedad, connotación u organización lo requieran, incluyendo operaciones cuyo origen o destino sea el exterior del país. El instructor penal es el encargado de solicitar al fiscal la aprobación para el empleo de dichas técnicas, mediante escrito en el que debe fundamentar la necesidad y el alcance de su aplicación a partir de las particularidades del hecho investigado, los participantes y peligrosidad, así como las razones que justifican su utilización.

Luego agrega que se entiende como investigación encubierta la realización de operaciones mediante el empleo de agentes encubiertos, entrenados por los órganos especializados del Ministerio del Interior para penetrar y mantenerse informados a fin de ejercer el control de las actividades delictivas de que se trate, con la utilización o no de otros recursos técnicos. Luego regula la exención de responsabilidad penal y el control judicial.

No tiene disposiciones específicas aplicables a la prueba electrónica más allá de esta cláusula de uso de recursos técnicos.

Por último, establece dicha Ley que se considera vigilancia electrónica o de otro tipo aquella en la que se utilizan medios cuya aplicación proporciona la escucha y grabación de voces, localización y seguimiento, fijaciones fotográficas y filmación de imágenes, intervención de las comunicaciones de cualquier tipo, acceso a sistemas computarizados y otros recursos técnicos que permitan conocer y demostrar el hecho delictivo.

La norma de entrega vigilada que refiere a permitir que mercancías, cargas, bultos postales u otras remesas ilícitas o sospechosas salgan del territorio de uno o más estados, lo atraviesen o entren en él, con el conocimiento y bajo la supervisión de sus autoridades competentes o con su intervención, con el fin de investigar delitos e identificar a las personas involucradas en la comisión de estos. También se emplean en operaciones ilegales realizadas dentro del territorio nacional.

Cabe señalar que todo este capítulo de técnicas especiales de investigación que hemos comentado fue reformado en 2019, dándose su redacción actual.

Panamá

Panamá posee estas medidas en varias leyes. En primer lugar, la Ley 16 de 2004 sobre Contribución a la prevención y eliminación de la explotación sexual comercial de personas menores de edad, posee en su art. 16 que el Ministerio Público podrá realizar operaciones encubiertas en el curso de sus investigaciones, con el propósito de identificar los autores, cómplices o encubridores, o para esclarecer los hechos relacionados con los delitos mencionados en el Título VI del Libro II del Código Penal. De igual manera, cuando existan indicios graves de la comisión de algunos de estos delitos, el Procurador General de la Nación podrá ordenar la intercepción y registro de las comunicaciones telefónicas, de correo electrónico o en foros de conversación a través de la red en las que participen las personas investigadas, con el objeto de recabar elementos de prueba relativos a tales delitos. Las transcripciones de las grabaciones constarán en un acta en la que solo se incorporará aquello que guarde relación con el caso investigado, la cual será refrendada por el funcionario encargado de la diligencia y por su superior jerárquico.

Luego en el art. 315 regula de manera muy genérica las operaciones encubiertas diciendo que el fiscal podrá practicar operaciones encubiertas, como compra controlada, entrega vigilada, análisis e infiltración de organización criminal y vigilancia y seguimiento de personas en el curso de una investigación, con el propósito de recabar evidencias para determinar la ocurrencia del hecho punible, así como sus actores y partícipes.

Por último, en la Ley 121 del 2013 sobre actividades relacionadas con el delito de delincuencia organizada, regula en art. 9 y subsiguientes las técnicas especiales de investigación, comenzando por las operaciones encubiertas y entregas vigiladas. Dichas disposiciones no poseen matices especiales aplicables a la prueba electrónica. De hecho, menciona para el agente encubierto la infiltración en el tráfico comercial, asumir obligaciones, ingresar y participar en reuniones en el lugar de trabajo, el domicilio o los lugares donde el grupo delictivo organizado lleve a cabo sus operaciones o transacciones.

Asimismo, dice que si el agente encubierto encuentra, en los lugares donde se lleve a cabo la operación, información útil para los fines de la operación, lo hará saber al fiscal competente encargado de la investigación para que este disponga el desarrollo de una diligencia para la recopilación de la información y los elementos materiales o evidencias físicas encontrados. Por ende no refiere puntualmente a evidencias electrónicas.

Respecto a la entrega vigilada refiere a remesas de drogas ilícitas, de precursores o sustancias ilícitas, dinero, armas u otros elementos ilícitos o sospechosos de contenerlos, o los bienes materiales, especies, objetos y efectos que se presumen ilícitos en posesión o destinados a personas o a un grupo u organización criminal, no refiriendo tampoco a lo digital.

Respecto a la vigilancia electrónica dice que en el marco de una investigación que permita presumir fundadamente que se está preparando u consumando un delito, el fiscal podrá ordenar a los agentes de policía realizar vigilancia y seguimiento de personas, grupos, organizaciones, vehículos, lugares y

objetos de cualquier naturaleza, con el propósito de verificar hechos, detalles, situaciones, vinculaciones o comportamientos útiles la investigación. La vigilancia y seguimiento pueden hacerse por cualquier medio, a pie o en vehículos terrestres, aéreos, marítimos o fluviales, inclusive utilizando equipos electrónicos u otros medios tecnológicos.

Perú

En el año 2015 Perú dictó el decreto legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado. El objetivo de dicha ley es fortalecer las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, a través del uso de las TICs.

Dicha ley regula el acceso de la Unidad Especializada de la Policía Nacional de Perú, en caso de flagrancia delictiva, a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos. A su vez pone en cabeza de los concesionarios de servicios públicos de telecomunicaciones el deber de brindar estos datos. Luego regula el mecanismo de convalidación judicial, así como qué datos se encuentran excluidos.

La Ley de Delitos Informáticos regula los delitos relacionados con la tecnología, pero también contiene algunas disposiciones procesales como el agente encubierto para esos delitos, equipos conjuntos para investigación e intercambio de información entre organismos encargados de la persecución penal. Modifica la Ley contra el Crimen Organizado.

En lo que respecta al agente encubierto, el art. 13 de la Ley contra el Crimen Organizado 30077, dice que los agentes encubiertos, una vez emitida la disposición fiscal que autoriza su participación, quedan facultados para participar en el tráfico jurídico y social, adquirir, poseer o transportar bienes de carácter delictivo, permitir su incautación e intervenir en toda actividad útil y necesaria para la investigación del delito que motivó la diligencia.

Impone el deber de colaboración y confidencialidad a todas las instituciones y organismos del estado, funcionarios y servidores públicos, así como las personas naturales o jurídicas del sector privado para la aplicación de la Ley.

La Ley de crimen organizado se aplica a más de 21 tipos de delitos (entre ellos los “delitos informáticos”) que sean cometidos por organizaciones criminales de tres o más personas. También regula las entregas vigiladas sin hacer referencia a evidencias electrónicas, disponiendo la circulación o entrega vigilada de cualquier bien relacionado a la presunta comisión de uno o más delitos vinculados a una organización criminal.

V. Aplicación de las leyes

Una vez llevado a cabo el establecimiento del marco normativo, la aplicación de la legislación en materia de prueba electrónica reviste una serie de particularidades que parten de su propio carácter heterogéneo. Si toda norma jurídica debe ser interpretada, como paso previo a aplicarla, de acuerdo con la realidad social del tiempo en que tiene que llevarse a cabo dicha aplicación, pocas normas en materia procesal penal están tan expuestas a la obsolescencia como la que nos ocupa. Así, si medios probatorios clásicos (v.gr: testificales, documentales…) pueden seguir regulándose por normas procesales que permanezcan invariables durante decenios, todo lo relacionado con la evidencia digital requiere una actualización constante. De ahí que el legislador deba permanecer especialmente vigilante si no quiere quedar sobrepasado por el estado de la técnica y que la función integradora o complementaria de la jurisprudencia cobre un especial relieve para ir adaptando las circunstancias sobrevenidas a aquellos huecos donde una interpretación literal de la Ley no es capaz de llegar.

Y es que, en materia de prueba digital, se requiere corporeizar la evidencia. A principios de este siglo, bastaba con obtención de una copia del dispositivo aprehendido, hecha a presencia del fedatario público, llevando a cabo el precinto del ordenador para asegurar su indemnidad en la custodia y la

posibilidad de someterlo a pericias en sede judicial. Sin embargo, si antaño solo existía interés por la cesión estática de mensajes producidos de forma electrónica, en la actualidad es especialmente relevante profundizar en la evidencia relacionada con la ocupación dinámica de todo tipo de datos. Así, en ocasiones la prueba puede recaer sobre datos cuyo tratamiento está automatizado, y encontrarse en instrumentos de almacenamiento masivo o bien estar deslocalizados -cloud computing-. Otras veces, lo relevante será otros extremos de la comunicación, como el acceso a determinadas fuentes de información o la ubicación referente a geolocalizaciones, e incluso su tratamiento cruzado -metadatos-. El flujo de información electrónica es constante y empieza a ser difícil de abarcar, en sintonía con el desarrollo tecnológico en la materia. Las ventajas que brinda esta vía suponen la apertura de nuevas líneas en la comisión de ilícitos penales que requieren una respuesta procesal en la lucha contra las nuevas formas de delincuencia.

Se parte de la premisa de que la información almacenada en soporte digital contiene un buen número de datos de carácter personal. De ahí que la aplicación de las normas deba empezar atendiendo al rango constitucional de los derechos en conflicto. Las diferentes Constituciones confieren distinto desarrollo al derecho a la intimidad de la persona, pero lo contemplan en todos los casos. Como emanación del mismo, el secreto de las comunicaciones, pueden referirse a las vías clásicas de comunicación o bien contemplar ya la posibilidad de que tengan lugar electrónicamente. En cualquier caso, la protección jurídica, necesariamente formal, es máxima, predicándose como un derecho del ciudadano para garantizar espacios de privacidad frente al estado. De ahí que el sacrificio que tenga que hacerse a este derecho en el seno de investigaciones criminales, tenga que estar especialmente avalado por el cumplimiento de las prescripciones legales que se establezcan. Con independencia de que el tratamiento constitucional de la intimidad pueda estar más o menos fragmentado en los distintos países, en todos los casos nos encontramos ante auténticas garantías para el ciudadano, no ante simples formalidades, de modo que la aplicación de la Ley debe evitar una intromisión injustificada en entorno digital de la persona investigada. Precisamente este ámbito de privacidad es lo que ha hecho que distintos códigos, como se pudo ver en el apartado precedente, tuvieran que incluir normas específicas relativas al ingreso, “allanamiento” de dispositivos informáticos regulando las características especiales tanto del registro como del secuestro de datos. La multifuncionalidad de los datos almacenados a los que nos referíamos anteriormente no obsta a que, en primer término y dada la naturaleza jurídica del derecho afectado, el operador jurídico que está en trance de aplicar la ley lo contemple de forma unitaria.

Una vez que se contempla la necesidad de salvaguardar el derecho constitucional, función que corresponde principalmente al legislador, pero también a la autoridad judicial en el momento mismo de la aplicación, los distintos textos procesales requieren de la observancia de una serie de principios para la producción regular de la evidencia, desde un punto de vista general y antes de considerar las diligencias de investigación concretas de las que se empieza a obtener la evidencia. Amén de las particularidades de cada sistema procesal, podemos poner el acento sobre principios rectores clásicos cuya concurrencia inicial puede empezar a garantizar el ajuste a Derecho de la prueba electrónica obtenida, haciéndonos eco de los apreciados por el legislador español en la importante reforma operada en su Ley de Enjuiciamiento Criminal en el año 2015[17]:

> *- Autorización judicial: corresponderá a la autoridad judicial o fiscal sobre la que recaiga la instrucción de la causa judicial en cada estado, la autorización para hacer uso de cualquier medio de investigación tecnológico con el que se pretenda obtener datos de relevancia penal para la investigación de la causa, impidiendo, así, que la fuerza policial obtenga por sí misma datos sensibles para la intimidad del investigado.*
>
> *- Principio de legalidad: la autorización anterior que habilite el uso de la medida invasiva del derecho fundamental no puede prestarse de forma caprichosa, sino tener expreso respaldo normativo. De una parte, el ciudadano tiene derecho a saber en qué circunstancias puede restringirse su secreto de las comunicaciones; de otro, se evitan situaciones de arbitrariedad por parte de los poderes públicos[18].*

17 Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.
18 TEDH. Caso Rotaru contra Rumanía, 4/05/2000.

- Principio de especialidad: desde una perspectiva positiva, la medida autorizada de la que se puede extraer la evidencia digital debe estar relacionada con un delito contrato. Y, en negativo, el seguimiento de este principio evitará diligencias prospectivas o la apertura de investigaciones carentes de base objetiva. La investigación debe ir enfocada a la búsqueda de una evidencia digital concreta, impidiendo el acopio de datos íntimos del investigado de los que, tal vez, resulte el hallazgo de una actividad delictiva sobre la que no existían indicios en el momento previo a la puesta en marcha de la investigación.

- Principio de idoneidad: con carácter previo a restringir el derecho fundamental, se reputa necesario valorar si el medio tecnológico a utilizar es útil al fin que se pretende obtener en la investigación, de modo que únicamente se haga uso de aquellos que resulten eficaces para empezar a conformar la evidencia electrónica en función de la telecomunicación empleada por el sujeto afectado y las posibilidades técnicas de los investigadores.

- Principios de excepcionalidad y necesidad: estando en juego un derecho fundamental, hay que valorar si los datos a obtener con el empleo de los medios limitativos de tal derecho se pueden conseguir con el uso de medidas menos gravosas que se presenten como igualmente útiles.

- Principio de proporcionalidad: como cualquier otra de investigación sometida a consideración del instructor, se llevará a cabo el juicio de ponderación entre el sacrificio temporal que comporta el uso de la medida para el derecho fundamental afectado por la misma y la existencia del interés público implícito en la necesidad de recabar pruebas por vía electrónica en el marco de un procedimiento penal. En ocasiones, los parámetros para llevar a cabo este juicio pueden venir definidos legalmente, y referirse a extremos tales como la gravedad del hecho, su trascendencia social, la intensidad de los indicios con los que se cuenten en el momento de la valoración o la relevancia del resultado que se persiga obtener.

El juicio ponderativo judicial, ya en concreto, se proyecta sobre el registro de los datos electrónicos. A su vez, en este registro, se aprecian distintas fases, de modo que la aplicación legal tendrá características en cada una de ellas: 1) Aprehensión del continente donde está la información; 2) Acceso o análisis de su contenido; 3) Incorporación de lo seleccionado tras su análisis al proceso.

Así, detectado el dispositivo de conectividad donde se halla el dato a investigar, se debe recabar la autorización judicial anteriormente indicaba para su ocupación. Esta autorización debe contener, necesariamente, una motivación individualizada en función del lugar donde se encuentre el dispositivo objeto de incautación, siendo habitual que se requiera una exposición diferenciada cuando, además del dato automatizado, se necesite acceder a un domicilio u otro espacio cerrado reservado al objeto de aprehender el ordenador o dispositivo de almacenamiento masivo que corresponda. Hay que subrayar aquí que el derecho al entorno digital de todo investigado no se presenta como una prolongación de la inviolabilidad domiciliaria, sino que la necesidad de la doble motivación viene impuesta por la naturaleza diferenciada de ambos derechos, aunque sean emanaciones de la intimidad del individuo.

En ocasiones puede suceder que existan razones de urgencia y necesidad que aboquen a un registro sin haberse recabado la previa autorización judicial. La regularidad procesal de estos supuestos requeriría de una regulación pormenorizada de los supuestos en los que estaría permitido, estableciéndose un régimen de comunicación inmediata y posterior sometimiento a revocación o confirmación en un lapso de tiempo perentorio. Todo ello reduciendo la labor policial previa a lo imprescindible, dada la injerencia en el derecho fundamental que supondría esta actividad aún no jurisdiccional.

En los supuestos donde se incauta un dispositivo electrónico fuera del domicilio del investigado, sucede que no suele haber una previa habilitación judicial para la aprehensión, que únicamente se interesa al hilo de una entrada y registro en domicilio. En este supuesto, el aplicador del derecho tiene que solventar dos problemas jurídicos que puede plantear la aprehensión. El primero es qué dispositivo incautar. En este caso, cuando la necesidad se suscita al hilo de una operación policial, será quien la ejecuta el que tendrá que decidir qué dispositivo concreto debe ser objeto de aprehensión, poniendo el hecho en conocimiento de la autoridad judicial para que la autorice, naciendo de forma sobrevenida la

misma obligación de motivación que cuando se inicia mediante una entrada domiciliaria. En segundo lugar, y partiendo de datos automatizados de carácter simple, se suscita la duda de si es factible que se lleven a cabo meros visionados superficiales del contenido del dispositivo para facilitar el análisis sobre la utilidad de su aprehensión. La respuesta debe ser necesariamente negativa, siendo estos "pantallazos" una intromisión ilegítima que puede viciar la investigación, debiendo estarse a las normas reguladoras de cualquier registro. Solo aplicando estas normas en cualquier tipo de aprehensión, se puede llevar a cabo el necesario juicio de razonabilidad por parte de quien tiene que efectuar la autorización, evitando ocupaciones de dispositivos que pueda tildarse de prospectivas y no razonables y respetando el derecho a la información privada del sometido a la investigación.

El punto de partida en la aplicación de la ley es que no existen autorizaciones implícitas ni mandamientos de intromisión en el espacio de exclusión, salvo que el sistema legal en cuestión así lo permita, fijándolo con suficiencia y claridad. Si a lo largo de cualquier investigación criminal se va perfilando el objeto de investigación y los extremos sobre los que versa la prueba digital, ya en el momento inicial debe empezar a acotarse el hecho punible y los dispositivos de los que se pretende extraer la información, de modo que la autorización de inspecciones oculares para averiguar un indeterminado y potencial comportamiento delictivo llevado a cabo por vía telemática, viene a contrariar alguno de los principios antes enumerados, con la consecuencia jurídica de la nulidad. De otro lado, una autorización judicial realizada en consonancia con tales principios y directrices legales, permitirá establecer ab initio las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, el sometimiento a las correspondientes pericias, minimizando las posibilidades de manipulación.

En relación a lo anterior, y dado el carácter no tangible de los datos que se obtienen mediante el empleo de la informática, en el momento mismo de la ocupación nace la obligación de fijar la cadena de custodia, de modo que el propio control jurisdiccional, vía autorización, debería fijar las medidas oportunas desde el momento mismo de la ocupación. Se trata de que, en un momento ulterior de la instrucción de la causa, lo ocupado coincida con lo analizado, por lo que en la aplicación de la Ley tiene especial trascendencia no perder de vista la fácil modificabilidad de los datos. De ahí que se practique como deseable la llevanza del aseguramiento de la integridad mediante labores de clonado, incluso llevándolo a cabo in situ en el momento de la aprehensión del dispositivo, con escrupuloso respeto de las garantías inherentes a todo registro, tales como la presencia de fedatario público y de la asistencia letrada de la defensa. Luego se puede reforzar la idea de la integridad de la cadena de custodia con garantías adicionales, en función de las posibilidades técnicas, llevando a cabo actividades procesales tales como el precinto de los equipos incautados, para su posterior apertura en sede judicial. En suma, la idea es dotar a los sistemas legales del máximo rigor en cuanto a la preservación de los datos aprehendidos y su integridad, evitando cualquier circunstancia que provoque su mutación, transformación o incluso desaparición, con la repercusión negativa en materia probatoria.

Y es que el conseguir el aseguramiento en las condiciones expuestas repercute directamente en fases procedimentales ulteriores, en lo que lo esencial es garantizar la previsión de reiterabilidad, sin que puedan cercenarse derechos tales como el sometimiento de los datos electrónicos a contrapericias, y asegurando su indemnidad hasta el momento posterior del plenario, donde se pueda reproducir la información electrónica con respecto a principios como el de contradicción. La intervención activa del fedatario judicial, actuando como garante de la legalidad, minimiza problemas con la cadena de custodia y grietas en el aseguramiento de la prueba.

Todo lo anterior evidencia que, aunque las distintas regulaciones aludan a la aprehensión del dispositivo de almacenamiento masivo o similares, la atención del aplicador se centra en el contenido, de modo que, una vez llevada a cabo la clonación, resulta hasta aconsejable que se proceda a alzar la ocupación del soporte físico de los archivos sometidos a investigación, previa verificación de la culminación del aseguramiento. Esta cuestión aborda tangencialmente el tema relativo al modo de llevar a cabo la ejecución del registro del dispositivo electrónico, tema sobre el que pronto tuvo ocasión de pronunciarse el propio TEDH[19], para considerar que una ocupación respetuosa con los derechos humanos requería

19 Caso Weiser y Bicos Beteiligungen GmgH contra Austria. 16/10/2007.

de la concurrencia de estos requisitos: 1) presencia de las partes, principalmente la del afectado o su defensa; 2) levantamiento de acta de las operaciones hechas en el registro, con inclusión de lista de bienes ocupados y ficheros inspeccionados, realizándose copia de seguridad bajo la garantía de tercero imparcial; 3) establecimiento de un derecho al usuario del dispositivo registrado de objetar sobre su aprehensión, decidiendo, en tal caso, el juez; 4) garantía adicional de un tercero imparcial suplementario en supuestos de registro de abogados en ejercicio, como refuerzo de su independencia profesional.

Todo lo expuesto incide en una idea, y es que la autorización y ejecución de los registros informáticos y de dispositivos electrónicos que contengan información posiblemente delictiva, se efectúen de forma selectiva, incluso en un momento inicial de la investigación, logrando reducir la injerencia en el entorno virtual del investigado.

Y para facilitar la incorporación de los datos al proceso, lo que constituiría la tercera y última fase en la aplicación de la ley, los distintos sistemas legales pueden articular deberes de colaboración informativa a observar por cualquier persona que conozca el funcionamiento del sistema informático, pudiendo establecer sanciones en caso de desatención de tal deber o articulando paralelamente obligaciones de guardar reserva a quienes intervengan en tales actuaciones. Resulta particularmente importante esta colaboración en materias tales como la obtención de claves de desbloqueo o código de desencriptación. En particular, cobra aquí relieve el juicio de ponderación que requiere la obtención de material probatorio electrónico, en la medida que deben arbitrarse deberes que no supongan una carga desproporcionada. Menos conflictivo será que la colaboración recaiga en titulares o responsables del sistema informático o bases de datos registrados, cuya asistencia en ocasiones se torna técnicamente imprescindible para la materialización del registro informático.

La particularidad de los datos que se contienen en equipo informáticos permite unas modalidades de injerencia acordes con los datos que se pretenden obtener, y que requieren también de una valoración por parte del operador jurídico para dotar al registro de regularidad procesal. Así, el examen del dispositivo electrónico puede efectuarse a distancia y sin conocimiento del titular, pudiendo dar lugar a dos formas de investigación: una, mediante el uso de datos de identificación y códigos o accesos duplicados -monitorización-, lo que supone la existencia de una suerte de administrador interconectado en red que vigila desde un puesto de control remoto ; y dos, mediante la instalación de un software espía, que permite que tal vigilancia se realice desde otro equipo informático, bien mediante ataques indiscriminados o bien mediante ataques selectivos. No son pocos los sistemas legales que ya prevén expresamente el análisis remoto de los equipos informáticos.

Cualquiera que sea la vía elegida de las expuestas en el párrafo precedente, el sometimiento a autorización judicial conlleva la consideración de dos distintas fases para su uso. La primera, englobaría la instalación del sistema o software, esto es, la autorización para la labor preparatoria inmediatamente anterior a la captación del dato automatizado. Y la segunda sería la activación y desactivación del sistema elegido para ejecutar el registro. Así, el registro tiene una doble vertiente, ya que se puede efectuar de forma remota, sin conocimiento del usuario y sin inmediatez, o bien como se llevaba a cabo tradicionalmente, en el que había un contacto directo entre el dispositivo y el usuario. De cualquier manera, es clara la distinción entre estas dos tipologías de registro y la interceptación de las telecomunicaciones, que tiene incidencia en la actividad a tiempo real del investigado.

Legislaciones avanzadas en materia de prueba electrónica prestan especial atención a este posible control remoto de los datos contenidos en dispositivos de almacenamiento masivo, limitando su posibilidad a delitos especialmente graves[20], o requiriendo una pena mínima de prisión aparejada al delito investigado. Como regla general, el acudir a esta medida requiere un control judicial reforzado, quizá motivado por el propio carácter volátil de los datos relevantes para la investigación, así como por la imposibilidad de que no se obtenga otra información de carácter privado del investigado, aunque posteriormente se descarte. Aunque se utilice la vía remota para la obtención de evidencia relacionada con una pluralidad de personas, se requiere inexcusablemente que el alcance de la medida de investigación contenga unas “menciones mínimas”[21], sin las cuales, y en caso de recaer sobre elemento esenciales de la prueba obtenida, puede viciar la misma de nulidad.

20 V.gr: Artículo 588 septies a) de la LECrim de España.
21 TEDH. Caso Modestou contra Grecia. 16/03/2017.

Como corolario de lo anterior, el operador jurídico que aplique la ley deberá permanecer vigilante a que no excedan los plazos de duración por los que la interceptación ha sido concedida. Y esto se predica tanto en el momento inicial, ajustando el plazo a la previsión temporal para la obtención de la evidencia, como en un momento posterior, en función de la marcha de la investigación, pudiendo cesarse la medida autorizada en el supuesto en que, aún no expirado el plazo, la observación de la telecomunicación ya haya durado lo imprescindible para la afectación del derecho del sometido a la investigación. En el momento de aplicar la medida, se requiere, igualmente, la determinación precisa del dies a quo desde el que se computa la injerencia, siendo este, normalmente, el de la instalación del dispositivo, y la posibilidad de activarlo. A partir de ese documento, y con independencia del carácter dinámico del registro, debe poder documentarse la información que se vaya obteniendo.

VI. Cuestiones prácticas

Los problemas prácticos que plantea la incorporación al proceso de la evidencia digital arrancan de la investigación policial misma. Y, aunque no es objeto específico del presente trabajo, la reunión mantenida con Interpol a través de su funcionario Adrián Acosta, puso de relieve algunas circunstancias que no se pueden soslayar a la hora de abordar este tema. Así, la iniciación de distintos proyectos (v.gr: CiberAmérica), puso de relieve la necesidad de capacitación de las unidades policiales que, de hecho, ejecutan las resoluciones judiciales de las que se extrae la prueba. No en vano, actuaciones tan aparentemente inocuas como apagar un ordenador pueden impedir la extracción del dato electrónico si está almacenado en la nube y hacer fracasar una investigación. De ahí que resulte esencial un manejo correcto y fluido de la Live Data Forensic System por parte de los cuerpos policiales que coadyuvan a las investigaciones criminales e inician, en suma, la obtención de la prueba electrónica.

Se necesita, no solo dotar a La Policía de los conocimientos necesarios en materia Procesal Penal, sino también suministrarles el software adecuado para la materialización de los allanamientos y obtención de los datos electrónicos. En un momento posterior, también es menester que la adecuada dotación de los medios técnicos, llegue hasta los laboratorios forenses. Uno de los problemas detectados procede de la inexistencia de las licencias necesarias para la homologación de las pericias, lo que puede suponer un conflicto de cara a sostener la validez de la prueba electrónica en el seno del procedimiento criminal. Se ha detectado, en numerosos países, como los peritos tienen que hacer uso de su propio software para la confección de los dictámenes periciales, lo que puede entrañar dudas en relación con su idoneidad. De hecho, la frecuente realización de los informes fuera de la sede de los órganos jurisdiccionales, también puede entrañar problemas que es menester resolver con una legislación que abarque estos supuestos. Así, en la práctica se han suscitado conflictos en relación a la necesidad de que las labores de clonación de datos electrónicos se lleven a cabo a presencia de letrado, o incluso en cuanto a la posible elección de perito[22].

La necesidad de llevar a cabo una adecuada capacitación, no atañe únicamente a las fuerzas policiales. Como no puede ser de otra manera, se precisa que el aumento exponencial de crímenes llevados a cabo de forma telemática, vaya acompañada de una formación específica en la Fiscalía y en la Judicatura, máxime cuando la insuficiente respuesta de la ley -como vinos en apartados precedentes- obliga a hacer un especial esfuerzo para que la jurisprudencia vaya dando respuesta a los problemas que plantee la evidencia digital. Partiendo de una necesidad de establecer protocolos de coordinación con La Policía y en función de los órganos que en cada estado asume la competencia objetiva para la persecución de los concretos delitos, la frecuente existencia de un elemento trasnacional en el crimen investigado exige un reforzamiento de los elementos de cooperación internacional y la necesidad de que los mecanismos que se instauren sean especialmente ágiles. Ejemplo del avance en esta materia es la colaboración de la Fiscalía de Paraguay en la operación Hades, que supuso la detención de un ciudadano alemán por tenencia y distribución de pornografía infantil y que se llevó a cabo el 12 de abril de 2021, con el cierre de una plataforma que operaba en la DarkNet.

22 Sentencia del Tribunal Supremo español número 165/2016, de 2 de marzo, Licitud de la diligencia de intervención de un ordenador, su apertura y la extracción del disco duro con el fin de que sea examinado y peritado por funcionarios policiales. La diligencia fue practicada con la intervención del Secretario Judicial. No es preceptivo que estuviera delante un perito nombrado por la defensa ni tampoco los letrados de los imputados, quienes además tampoco lo interesaron cuando la juez acordó por providencia la práctica de esas diligencias.

De forma específica, se han planteado problemas con la práctica policial consistente en el ciberpatrullaje por fuentes abiertas, por entrar en colisión con el principio de especialidad. Se trata, en suma, de navegar por internet y obtener indicios de la comisión de delitos que aún no están siendo investigados. Figura muy distinta a la del agente encubierto digital, habilitado por una resolución judicial previa para infiltrarse en un canal cerrado de la red, y llevar a cabo una tarea específica que puede ser delictiva, y cuya validez ha sido avalada por la distinta jurisprudencia[23], poniendo de relieve su carácter excepcional y siempre que no suponga provocación para la comisión del delito. Menor atención presta legislación y Tribunales a la entrega vigilada digital. De hecho, el Convenio de Budapest no se refiere a esta materia. Se trata de una técnica de investigación clásicamente dirigida a los procedimientos relativos al narcotráfico, en los que la entrega se materializa de forma física en sustancias psicotrópicas o drogas tóxicas, pero que podría resultar extrapolable a entregas de contenido digital cuando se trate de bienes susceptibles de estar en este formato -por ejemplo, archivos relativos a pornografía infantil- o aquellos cuya entrega se puede monitorear digitalmente.

En el plano legislativo, las distintas iniciativas legislativas deberían ponderar la conveniencia de superar el principio de territorialidad que, para ocupación de información, parece extraerse del Convenio de Budapest[24]. Dada la naturaleza de la información electrónica, no resulta sencillo saber geográficamente dónde está almacenada de manera concreta. La concatenación de servidores, que replican los datos electrónicos, dificulta la aplicación de esta norma. Se antoja más relevante tomar en consideración si existe un acceso técnico posible desde un dispositivo que haya sido espacialmente aprehendido en un estado y desde el que se haya hecho uso de los permisos que posibiliten el acceso a la información con relevancia penal, especialmente cuando se trata de un almacenamiento desmoralizado -cloud computing-. El acogimiento de la territorialidad por la que se aboga desde el Consejo de Europa, remite a una cooperación jurídica internacional aún en fase embrionaria. En nada se resiente el principio de soberanía si el acceso a la información albergada en un tercer país se castiga desde el que se materializa el acceso y se lleva a cabo la aprehensión, con salvaguarda de los derechos fundamentales de ese estado[25]. El entorno digital del ciudadano de 2001 en poco se parece al actual, por lo que hay que dar respuesta a la ampliación del mismo, con la apertura de nuevas vías con las que perpetrar conductas delictivas.

Establecida la Ley y vistos en el apartado anterior los parámetros que pueden tenerse en cuenta a la hora de su aplicación, respetando las particularidades de cada sistema legislativo, los problemas probatorios aparecen pronto. Uno de ellos, podría ser el de la aportación por el particular de efectos tecnológicos, a veces acompañado de una pericia. En este caso, la intervención de los cuerpos policiales y los peritos adscritos al Juzgado seguiría siendo necesaria con posterioridad a la aportación, en aras a verificar las garantías de la ocupación de los datos electrónicos y su contrastado. No obstante, se puede producir una quiebra en la cadena de custodia que requeriría tasar los supuestos de admisibilidad de esta prueba particular. Precisamente la fácil modificación y destrucción de los datos electrónicos, conlleva que dicha cadena cobre especial relevancia en este ámbito, lo que ha merecido ya una concreta alusión en algunos cuerpos normativos[26] y el análisis de la eventual nulidad de un peritaje por posible inobservancia en la integridad de la cadena[27].

También entrañan problemas de validez los llamados hallazgos casuales, especialmente si son heterogéneos, esto es, investigándose un delito, se encuentran datos electrónicos que suponen indicios de la comisión de otro que afecta a un bien jurídico totalmente distinto. Lo recomendable, en este punto, sería el establecimiento de criterios legales objetivos que permitan evaluar si la protección social

23 En Argentina, Juzgado de Primera Instancia en lo Penal, Contravencional y de Faltas N° 18, Caso 13.247-00/17, “Gigatribe Karatekick s/art. 128, párr. 1o CP”, 10 de abril de 2018; en España, Sentencia del Tribunal Supremo número 345/2019, 7 de febrero.
24 Artículo 32 b Una Parte podrá, sin la autorización de otra Parte: Tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.
25 En este sentido, Tribunal de distrito de los Estados Unidos para el distrito del este de Pennsylvania, orden de allanamiento No. 16-960-M-01 a Google, 19 de octubre de 2017, consideró que no se invade la soberanía de ningún estado si dicha empresa tecnológica aporta información almacenada en servidores extranjeros, al materializarse la invasión de la privacidad dentro del territorio de EEUU y no existir incautación alguna, al no privar al afectado de los correos o mensajes cuya transferencia se acuerda.
26 v.gr: Artículos 90 inc. e) y 150 del Código Procesal Penal Federal de Argentina, aprobado mediante ley 27063.
27 v.gr: Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal de la Capital Federal - Causa n° 46.744, “Fiscal s/ apela declaración de nulidad de informe pericial – Ricardo Jaime”, 24 de mayo de 2012, declaró la nulidad de un peritaje al constatarse la imposibilidad de aseverar que las computadoras secuestradas contuvieran los mismos archivos que los que albergaban en el momento del registro; Tribunal Supremo, Sala de lo Penal, sentencia número 429/2019. 27 de septiembre de 2019, avaló la validez de una apertura de sistemas informáticos, a pesar de no existir acta de precinto previa, al no haberse provocado ruptura alguna de la cadena de custodia

debe prevalecer sobre la individual del investigado afectado. El principio de proporcionalidad puede permitir la validación de hallazgos casuales cuando los datos descubiertos afecten a la comisión de un delito de suma gravedad, pero para impedir el menoscabo de derecho fundamental alguno y la nulidad del medio probatorio, parece aconsejable prever estos supuestos. Se trata de un tema, además, que ya ha sido tratado por la jurisprudencia, en la que se atiende a los márgenes de la orden judicial de allanamiento para dejar fuera la recogida de aquellos indicios que exceden del que figura como objeto de investigación en la resolución[28].

El uso cotidiano de los teléfonos móviles y el aumento de sus características técnicas, hace que cada vez sea más frecuente su utilización para albergar información digital que, en ocasiones, pueden suponer la evidencia de la perpetración un delito. Esto permite que haya que detenerse en si es factible el desbloqueo de teléfonos mediante el ingreso compulsivo de datos biométricos. En ocasiones, la decisión ha pasado por valorar el eventual carácter testimonial o revelador del pensamiento de la medida autorizada[29]; en otras, se ha prestado atención al principio de proporcionalidad, avalándose injerencias moderadas en el derecho a la intimidad cuando se trata de la investigación de delitos graves[30].

Por tanto, la práctica cotidiana pone de relieve la celeridad con la que proliferan las nuevas tecnologías y la perpetración de los delitos cometidos mediante el empleo de las mismas. En un tiempo prudencial, no será extraño plantearse la necesidad de introducir tipos penales relativos al uso de drones. Al no ir en paralelo tal desarrollo tecnológico con la regulación legislativa en la materia, corresponderá al operador jurídico ir dando respuesta a la necesidad de producir evidencias digitales partiendo, en muchos casos, de la yuxtaposición con las normas que disciplina los medios probatorios tradicionales.

VII. Cooperación jurídica internacional

En el apartado de cooperación judicial, pretendemos analizar si los países de Latinoamérica adherentes al programa EL PAcCTO están habilitados con leyes que permitan cooperar de manera adecuada con otros países con respecto a la obtención de prueba electrónica.

Resulta primordial establecer si los países del programa EL PAcCTO están vinculados a tratados internacionales, ya sean bilaterales (con otros países, como suele ocurrir mucho en Américas) o multilaterales. Por este motivo, el cuestionario incluyó preguntas para determinar si los países tienen en vigor tratados multilaterales o bilaterales que permitan la cooperación judicial en la obtención de pruebas electrónicas. Además, se procuró saber qué medidas específicas incluyen dichos tratados referidos a la prueba electrónica o digital.

En temas de cooperación en ciberdelito y pruebas digitales, la referencia marco, a nivel mundial, es el Convenio de Budapest, al cual se incorporaron ya una tercera parte de los países miembros de Naciones Unidas. En la fecha en que se escribe este trabajo, el Convenio de Budapest ha sido ratificado por 66 países, pero otros 11 estaban en el proceso de accesión o ratificación.

En Latinoamérica, son ya muchos los países que se incorporaron al Convenio de Budapest. Así ocurrió ya con Argentina (2018), Chile (2017), Colombia (2020), Costa Rica (2018), República Dominicana (2013), Panamá (2014), Paraguay (2018) y Perú (2019). Guatemala, México y Brasil están presentemente en el proceso de accesión.

Es, por lo tanto, natural que, en las respuestas a las cuestiones, un buen número de países refirieran, en cuanto a tratados internacionales, que están vinculados al Convenio de Budapest.

---

28 v.gr: En Argentina, Cámara de Apelaciones en lo Penal, Contravencional y de Faltas Caso N.o INC 2134/2018-1, 26 de septiembre de 2018; Décimo Circuito Judicial de Estados Unidos, caso Nro. 98-3077 United States o vs. Carey, 14 de abril de 1999.
29 Segundo Circuito Judicial del Estado de Virginia, caso CR-14-1439 Commonwealth of Virginia v. David Charles Baust, 28 de octubre de 2014, en el que se autorizó la colocación de la huella del encausado para desbloquear su teléfono, pero no se le obligó a entregar su clave de acceso o código de desbloqueo.30 El Tribunal Supremo español, en el, Auto núm. 3/2020, de 16 enero, consideró válida la obtención del código PIN de un teléfono móvil facilitada voluntariamente por los investigados al permitírsele realizar una llamada mientras estaban detenidos, aún sin presencia letrada; Juzgado Federal de Dolores, Causa FMP n° 88/2019 caratulada “Marcelo D’Alessio y otros s/ asociación ilícita y otros", 21 de febrero de 2019, consideró que el desbloqueo del terminal mediante lectura de rostro o huella dactilar resulta razonable, necesario, proporcional y pertinente al fin investigado y no comporta invasión corporal alguna.
30 El Tribunal Supremo español, en el, Auto núm. 3/2020, de 16 enero, consideró válida la obtención del código PIN de un teléfono móvil facilitada voluntariamente por los investigados al permitírsele realizar una llamada mientras estaban detenidos, aún sin presencia letrada; Juzgado Federal de Dolores, Causa FMP n° 88/2019 caratulada “Marcelo D’Alessio y otros s/ asociación ilícita y otros", 21 de febrero de 2019, consideró que el desbloqueo del terminal mediante lectura de rostro o huella dactilar resulta razonable, necesario, proporcional y pertinente al fin investigado y no comporta invasión corporal alguna.

En cuanto a instrumentos específicos de la región, si bien hubo alguna iniciativa en el pasado, sobre todo en el contexto de COMJIB[31], la verdad es que no está en vigor ningún tratado multilateral que regule de manera especial el tema de ciberdelito o la obtención de prueba electrónica. Sin perjuicio de ello, los mecanismos de cooperación vigentes no excluyen la prueba electrónica por lo que pueden ser utilizados en los que resulta aplicable.

Algunos países también ratificaron algunos instrumentos regionales sobre cooperación jurídica internacional en materias penales.

Así, la Convención Interamericana sobre Asistencia Mutua en Materia Penal, ratificada por Argentina (1996), Bolivia (1997), Brasil (2007), Chile (2008), Colombia (2003), Costa Rica (2012), Ecuador (2002), El Salvador (2004), Guatemala (2003), Honduras (2006), México (2003), Nicaragua (2002), Panamá (2002), Paraguay (2004), Perú (1995), Uruguay (2012) y Venezuela (1996). Su protocolo facultativo (el Protocolo relativo a la Convención Interamericana sobre Asistencia Mutua en Materia Penal) fue, por su turno, ratificado por Brasil (2007), Chile (2008), Colombia (2003), Ecuador (2002), Honduras (2006) y Paraguay (2004).

Hay, además, que referir un significativo número de tratados multilaterales en temas de asistencia mutua en asuntos penales, firmados en el contexto de Mercosur y de SICA.

Cabe destacar que algunos de los países se incorporaron a instrumentos internacionales de espectro más amplio.

Es el caso la Convención de la Naciones Unidas contra la Delincuencia Organizada Transnacional (la conocida UNTOC), la cual, si bien no se enfoca en ciberdelito, contiene algunos aspectos procesales que pueden ser utilizados para investigar ciberdelito y para cooperar internacionalmente en la obtención de pruebas electrónicas.

En Latinoamérica, esta convención fue ratificada por Argentina (2002), Bolivia (2005), Brasil (2004), Chile (2004), Colombia (2004), Costa Rica (2003), Cuba (2007), Ecuador (2002), El Salvador (2004), Guatemala (2003), Honduras (2003), México (2003), Nicaragua (2002), Panamá (2004), Paraguay (2004), Perú (2002), Uruguay (2005) y Venezuela (2002).

En cuanto a normas internas nacionales, en temas de cooperación internacional, en muchos de los países de Latinoamérica no existe un marco legal.

Por lo tanto, tampoco existen marcos legales específicos que permitan a los países cooperar con otros países específicamente en temas de ciberdelito o de obtención de pruebas electrónicas.
Así, que, en muchos casos, la cooperación se rige apenas por los instrumentos internacionales que los países tengan firmado y ratificado.

En este enfoque, toma dimensión, sobre todo, la Convención Americana sobre Asistencia Mutua en Materia Penal, que es un tratado multilateral que permite a las autoridades judiciales de un buen número de países de las Américas cooperar con autoridades de otros países.

En todo caso, la no existencia de marcos legales internos que regulen la cooperación internacional es una brecha muy importante, con consecuencias más amplias, más allá de la ciberdelincuencia. Quizás merezca un enfoque más amplio, que no solo se centre en el ciberdelito y las pruebas electrónicas.

31 En el año 2014, COMJIB aprobó el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia (https://ficp.es/wp-content/uploads/CONVENIO-CIBERDELITO-VERSION-A-LA-FIRMA.pdf). Este Convenio se aprobó en Madrid, en mayo de 2014 (https://www.segib.org/paises-iberoamericanos-firman-en-madrid-convenio-y-recomendacion-sobre-ciberdelincuencia/). Sin embargo, dicho convenio no está en vigor, ya que apenas fue ratificado por Cuba (https://comjib.org/ratificacion-de-la-republica-de-cuba-del-convenio-iberoamericano-de-cooperacion-sobre-investigacion-aseguramiento-y-obtencion-de-prueba-en-materia-de-ciberdelincuencia/) y por Nicaragua (http://ilo.org/dyn/natlex/natlex4.detail?p_lang=fr&p_isn=110734&p_count=97608).

Conclusiones

Resulta evidente la importancia que ha adquirido la evidencia electrónica o digital en la actividad jurídica y de los tribunales en la actualidad. Entendemos que, en el marco de los procesos penales, la evidencia digital está reemplazando paulatinamente a la evidencia física como medio de prueba para acreditar innumerables situaciones de hecho[32]. Este proceso de cambio trascendental para el proceso penal que ya había comenzado hace años se ha acelerado de manera vertiginosa con el COVID, generando la necesidad de adecuar tanto las normas como las prácticas jurisprudenciales y la capacitación de los operadores del sistema. Tal como hemos resaltado, la evidencia digital ya no está vinculada solo a los delitos informáticos, sino que resulta fundamental para la eficiencia en la investigación y tratamiento judicial de cualquier delito.

Puede afirmarse que los países de la región no cuentan con legislación adecuada para hacer frente a este nuevo desafío, quizá uno de los fundamentales para determinar los niveles de eficiencia y garantías del proceso penal en el futuro. Entendemos, por lo tanto, que resulta fundamental revisitar la legislación procesal penal de los países miembros de EL PAcCTO, con miras a determinar si están, o no, dotadas de un marco normativo apropiado para la obtención de prueba electrónica con la finalidad de ser utilizada en cualquier proceso penal. Y, en caso contrario promover las reformas necesarias.

En materia procesal, al igual que en la gran mayoría de los países de América Latina, los códigos procesal penales modernos vigentes en la mayoría de los países analizados, están basados en la idea de un sistema acusatorio. Estos códigos han sido implementados en la región en un importante movimiento iniciado en la década de los 90's sobre la base de las propuestas del Código Procesal Penal Modelo para Iberoamérica. Este origen normativo común facilita el intercambio de ideas entre los países de la región y permite que se compartan y aprovechen, entre los distintos países, la doctrina jurídica y las tendencias de la jurisprudencia.

Sin embargo, en general, ninguno de estos códigos incluye normas sobre evidencia electrónica. Todos fueron pensados antes de la aparición de la prueba digital y, por lo tanto, en general, todavía no incluyen las herramientas procesales adecuadas a la obtención de prueba digital o que tengan en cuenta las necesidades específicas de la prueba digital.

La circunstancia de que las legislaciones sean muy similares facilita la idea de pensar en desarrollar y proponer herramientas procesales para la evidencia digital que sean reguladas de manera similar. Es decir, el contexto de similitud de los códigos de la región permite un marco adecuado para que las cuestiones legales relevantes se debatan en conjunto. Es que este estándar procesal común a muchos países de América Latina facilita la discusión a nivel regional. Existe, por lo tanto, un campo de acción para pensar un marco normativo común a la región: la forma y validez de la obtención de pruebas electrónicas en proceso penal, los medios de prueba y obtención de pruebas, las medidas a nivel nacional, las medidas de cooperación internacional o la obtención transfronteriza de pruebas.

La verdad es que una legislación homogénea en lo que se refiere a los poderes procesales para la obtención de evidencia digital redundará también en una mejor cooperación internacional en materia penal.

---

32 A modo de ejemplos sencillos, si hasta hace poco tiempo para acreditar la presencia de un sospechoso en el lugar de los hechos se recurrió a la prueba testimonial de personas que hubieran estado en el lugar, hoy resulta más sencillo y fiable recurrir a datos de geolocalización de dispositivos o registros digitales de cámaras de seguridad; si para determinar si varias personas se conocían y tienen un alto grado de vinculación compatible con algún tipo de organización delictiva era necesario recurrir a diferentes medios de prueba que llevaba mucho tiempo recabar (testigos, informes, seguimientos, intervención de comunicaciones telefónicas, etc.) hoy el uso de OSINT analizando redes sociales o datos de comunicaciones y geolocalización permite en algunos supuestos el mismo resultado con menores recursos.

Por otro lado, importará introducir un marco adecuado de garantías procesales, especialmente considerando que este tipo de medidas es intrusivo y pueden poner en peligro el secreto de las comunicaciones, la privacidad, la vida personal y familiar, la libertad de expresión. Por lo tanto, una discusión de este tipo, al nivel regional, también tendrá impacto en un adecuado régimen de garantías, atendiendo especialmente al grado de intromisión importante que los medios de prueba en entornos digitales pueden significar para la intimidad y privacidad de los ciudadanos.

Se cree que este enfoque conjunto puede crear enormes sinergias: iniciativas conjuntas, por ejemplo, de capacitación, análisis conjunto de jurisprudencia, entre muchas otras.

El texto del ya mencionado Convenio de Budapest reúne un conjunto de normas penales y procesales cuya utilidad ha sido probada por la experiencia del derecho comparado de todos los países que lo han usado como modelo. Constituye un mínimo normativo sobre la materia que puede ser complementado con nuevas herramientas de acuerdo con las necesidades y características normativas de cada país. En este sentido, tomar como base de los proyectos normativos el texto del Convenio de Budapest como estándar mínimo, agregando aquellas cuestiones novedosas en materia de nuevas herramientas de investigación de acuerdo con las necesidades de cada país, resulta un paso fundamental en el desarrollo normativo de la prueba digital en estos países.

Importa añadir que está en su fase final de aprobación el Segundo Protocolo Adicional al Convenio de Budapest que, específicamente, introducirá nuevas normas con respecto a la obtención de evidencia digital, en particular en el extranjero o en la nube.

Por último, y en lo referido a técnicas especiales de investigación, son pocos los países que cuentan con legislación específica, siendo menester incorporar técnicas especiales que hagan frente al avance de las técnicas criminales cada vez más complejas. Fundamentalmente las técnicas de anonimato en la navegación, la utilización de encriptación, el alojamiento de datos en la nube, el uso de la Deep Web con fines ilícitos, etc. ha generado la necesidad de contar con medios de investigación que por su alto grado de incidencia en la intimidad requiere de una adecuada regulación que atendiendo las necesidades de la investigación penal pero en un marco de protección de los derechos humanos y con especial cuidado de la intimidad, el secreto de las comunicaciones y la libertad de expresión en medios tecnológicos.

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

EL PAcCTO es un programa de cooperación internacional financiado por la Unión Europea que persigue promover la seguridad ciudadana y el Estado de derecho en América Latina a través de una lucha más efectiva contra el crimen transnacional organizado y de una cooperación fortalecida en la materia. Cubre los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela. Es la primera vez que un programa regional europeo trabaja en toda la cadena penal para fortalecer la cooperación a través de tres componentes (cooperación policial, cooperación entre sistemas de justicia y sistemas penitenciarios) con cinco ejes transversales (cibercrimen, corrupción, derechos humanos, género y lavado de activos).

Programa liderado por
FIIAPP COOPERACIÓN ESPAÑOLA
EXPERTISE FRANCE

Socios coordinadores
iila
CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL
MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS

PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA