Artículo original

Evidencia digital y proceso penal paraguayo
Digital evidence and the Paraguayan criminal process
Digital rapykuere ha proceso paraguayo paraguayo

*María Del Carmen Palazón Ambrasath
https://orcid.org/0009-0004-4296-9466
Universidad Nacional del Nordeste. Corrientes, Argentina.

Resumen

La evidencia digital en el procedimiento penal es una realidad imposible de eludir. Abordar desde las garantías constitucionales, revisarlas a partir de los convenios internacionales e intentar comprender su alcance en la legislación penal paraguaya, es un doble juego de comprensiones que exige reconocimientos de los instrumentos internacionales y nacionales involucrados. A su vez se encuentran plasmados en el Plan Nacional de ciberseguridad y cibercrímenes adoptado o proyectado por el Paraguay, al que se sumaron la creación del departamento de Cibercrimen en la Policía Nacional y la Unidad Especializada de Delitos Informáticos del Ministerio Público. Tiene como objetivo abordar las estrategias nacionales de ciberseguridad y el rediseño de las estructuras estatales que combaten estos ciberdelitos. La investigación, optó por un enfoque cualitativo de tipo descriptivo, con diseño no experimental, para la recolección de datos utilizó el análisis documental. Se concluye que, el centro jurídico de toda evidencia digital se da con la ratificación del Convenio de Budapest, que define los datos de tráfico, establece los mecanismos para su obtención y conservación, por otro lado, se presenta la casuística a la expectante adhesión al segundo protocolo adicional del Convenio de Budapest, lo que significará la extraterritorialidad de la obtención de datos de tráfico. Se resalta que, el procedimiento penal paraguayo cuenta con estas herramientas, las cuales deben ser utilizadas por los operadores de justicia en cumplimiento de las garantías y libertades constitucionales, por lo que, el desarrollo jurisprudencial es de vital trascendencia.

Recibido: 03/10/2024 Aceptado: 03/03/2025 Publicado: 30/05/225

Resumen de artículo en el marco del Doctorado de la Universidad Nacional del Nordeste de Argentina.

*Doctoranda de la Universidad Nacional del Nordeste. Corrientes, Argentina.
Email: mariadelcarmenpalazonambrasath@gmail.com

Abogada y Notaria Pública por la Universidad Nacional de Asunción. Magíster de la Universidad Nacional de Itapúa. Doctoranda de la Universidad Iberoamérica. Doctoranda de la Universidad Nacional del Nordeste. Corrientes, Argentina. Agente fiscal en lo penal del Ministerio Público.

ISSN 2415-5063 Versión impresa ISSN 2415-5071 Versión en línea
https://ojs.ministeriopublico.gov.py Contacto: revistajuridica-isemp@ministeriopublico.gov.py

Palabras claves: ciberdelincuencia, evidencia digital, procedimiento penal, tráfico de datos, sistema informático.

Abstract

Digital evidence in criminal procedure is a reality impossible to avoid. Approaching from constitutional guarantees, reviewing them from international conventions and trying to understand their scope in Paraguayan criminal legislation, is a double set of understandings that requires recognition of the international and national instruments involved. In turn, they are embodied in the National Cyber security and Cybercrime Plan adopted or projected by Paraguay, which was joined by the creation of the Cybercrime Department in the National Police and the Specialized Unit for Cybercrimes of the Public Prosecutor's Office. It aims to address national cyber security strategies and the redesign of state structures that combat these cybercrimes. The research was based on a descriptive qualitative approach, with non-experimental design and the data was collected by documentary analysis. It is concluded that the legal center of all digital evidence is given with the ratification of the Budapest Convention, which defines the traffic data, establishes the mechanisms for its collection and preservation, on the other hand, the casuistry is presented to the expected adoption to the second additional protocol to the Budapest Convention, which will mean the extraterritoriality of the collection of traffic data. It is highlighted that the Paraguayan criminal procedure has these tools, which must be used by the operators of justice in compliance with the constitutional guarantees and freedoms, and therefore, the development of jurisprudence is of crucial importance.

Key words: cybercrime, digital evidence, criminal procedure, data trafficking, computer system.

Ñemombyky

Pe digital rapykuere procedimiento penal- peguágui, ndaikatúi oñekañývo. Kóvare oñeñe'ẽta ojehechakuévo umi garantía oĩva leiguasúpe, ojejesarekóta umi convenio internacional-re ojekuaa haguã mba'éichapa opoko ñande leikuéra paraguái peguáre, mokõi hendáicha ojekuaáta, tenonderã ojekuaáta umi kuatia ambue tetãmegua ha upéi kuatiakuéra ko ñane retãmegua. Upéicha avei kóva ojejuhu voi pe Plan Nacional de ciberseguridad-pe ha cibercrímenes omo ĩ va'ekue Paraguái, ha upérõ ojejapova'ekue pe departamento de Cibercrimen opytáva Policía Nacional ha Unidad Especializada de Delitos Informáticos, opytáva Ministerio Público-pe. Ojeheka umi estrategia ciberseguridad rehegua ha estado omohendava'ekue ohapejokóva ko'ã ciberdelitos. Ko investigación oiporavo enfoque cualitativo, tipo descriptivo, iñemohendapy katu no experimental, ombyatypa haguã dato oikotevẽva katu oiporu kuatiañe'ẽ oñehesa'ỹijómava. Oñembyapu'ávo oje'e pe digital rapykuere ipyrendaha Convenio de Budapest rehe, upépe omyesakã dato-kuéra omohenda umi mecanismo ojegueréko ha oñeñangareko haguã hese, ha avei, ojehechauka pe upe oñeha'arõitéva protocolo mokõiha omoirũva pe Convenio de Budapest-pe, péva he'ise ojejapyhara hague ambue terãre ojejuhu haguã ko'ã dato. Tekotevẽ ojekuaami pe procedimiento penal paraguayo oguerekopaha umi tembiporu ha tekotevẽva oiporu oĩvéva omba'apóva tekojorarãre ogarantisa haguã ñande leiguasu pu'aka, ha upévagui iporã tokakuaa pe jurisprudencia.

Ñe'ẽ tee: ciberdelincuencia, Digital rapykuere, procedimiento penal.

Introducción

Abordar la evidencia digital y el proceso penal paraguayo, implica necesariamente comenzar por revisar las garantías y libertades constitucionales del país. Cimentar con ellas y a partir de ellas cualquier revisión, garantizará el norte adecuado de cualquier interpretación.

El Paraguay a través de lo que denominó: Plan Nacional de Ciberseguridad, estableció las bases para una transformación digital segura para el país. Actualmente, se habla Gobierno Electrónico y un proceso de digitalización en el país, en el marco de una política pública de estrategia nacional en ciberseguridad y cibercrímenes.

Como parte de dicho plan nacional, se estableció en la Policía Nacional un Departamento de Cibercrimen y Lucha contra los Delitos Informáticos y el Ministerio Público estableció la Unidad Especializada de Delitos Informáticos. Siempre como parte del proyectado plan, se adoptó por ley nacional el Convenio sobre la Ciberdelincuencia de Budapest y su primer protocolo adicional.

Por medio del mencionado convenio se tipificó el delito de difusión de material racista y xenófobo a través de sistemas informáticos. El convenio cuenta con todo un procedimiento para la conservación, registro, confiscación, obtención en tiempo real de datos de tráfico y junto con este procedimiento detallado, la obligación de mantener en secreto estos procedimientos. Todos y cada uno de ellos con vigencia dentro del territorio nacional paraguayo, en atención al consagrado principio de territorialidad en el proceso penal.

Sin embargo, el segundo protocolo adicional sobre ciberseguridad plantea la extraterritorialidad de la captación y conservación de datos de tráfico, datos de los abonados y el acceso al registro de nombres de dominio, para la persecución penal de hechos punibles al igual que la posibilidad de castigar a los proveedores de servicios de internet que se encuentren en jurisdicción extranjera. Esta nueva base jurídica aún no se encuentra en vigencia, pero, ya plantea discusiones doctrinarias en la comunidad europea, en este trabajo se revisa brevemente la doctrina española al respecto.

Son innegables los esfuerzos del Ministerio Público en materia de delitos informáticos, pero, el mayor trabajo corresponderá a la Sala Penal de la Corte Suprema de Justicia o bien, a la Sala Constitucional de la misma, para la correcta armonización de procesos y garantías en la obtención de evidencia digital.

En este orden de consideraciones cabe preguntarse, ¿Son suficientes los mecanismos legales que el Paraguay posee para una adecuada obtención, registro, confiscación e incluso obtención de datos de tráfico en tiempo real, manteniendo, incluso, este procedimiento en secreto? Este trabajo de investigación tiene, por tanto, como objeto esencial responder esta pregunta y al efecto se abordarán las estrategias nacionales de ciberseguridad y el rediseño de las estructuras estatales que combaten estos ciberdelitos.

La evidencia digital desde la norma constitucional paraguaya

La norma constitucional bajo su Título II, De los derechos, de los deberes y de las garantías, en su Capítulo II, De la libertad, art. 33 sostiene:

> Del derecho a la intimidad. La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público

establecido en la ley o a los derechos de terceros, estará exenta de la autoridad pública. Se garantiza el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas (Intercontinental, 2000).

Igualmente, en su art. 36 dice:

Del derecho a la inviolabilidad del patrimonio documental y de la comunicación privada. El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas, cablegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos especialmente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio. En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado (Intercontinental, 2000).

Los arts. 33 y 36 de la norma fundamental necesitan integrarse intranormativamente con el art. 9 del Capítulo II, De la libertad, del Título II, De los derechos, deberes y de las garantías, que versa: «De la libertad y de la seguridad de las personas: Toda persona tiene derecho a ser protegida en su libertad y en su seguridad» (Intercontinental, 2000).

Corresponde apuntar aquí lo sostenido por Susanna Oromí i Vall-llovera (2020), cuando refiere:

> …no hay ninguna duda que el acceso y obtención por autoridades policiales o judiciales, en el marco de investigaciones penales, de datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, representan una injerencia en los derechos fundamentales garantizados (Oromí i Vall-llovera, 2020, págs. 1-13).

Sin embargo, aclara que, «…tal injerencia únicamente puede autorizarse para luchar contra la delincuencia grave» (Oromí i Vall-llovera, 2020, págs. 1-13). La citada autora, concluye sosteniendo que, en todo caso:

> …que lo importante para poder decidir si se debe autorizar el acceso y obtención de datos personales conservados por proveedores de servicios de comunicaciones electrónicas es el juicio de proporcionalidad que debe realizar el juez de instrucción, valorando, de un lado, la gravedad de la injerencia en los derechos fundamentales y, de otro, la gravedad de los hechos delictivos (Oromí i Vall-llovera, 2020, págs. 1-13).

Juan Carlos Ortiz Pradillo (2020), sostiene:

> En la construcción del Espacio Europeo de Libertad, Seguridad y Justicia, una de las grandes controversias aún por resolver se centra en cómo cohonestar las enormes posibilidades que la tecnología ofrece en materia de tratamiento informático de datos personales a gran escala (Big Data) y su empleo para la protección de la seguridad pública, la defensa o el orden público con la debida protección de los derechos fundamentales de

los ciudadanos reconocidos en el Convenio Europeo de los Derechos Humanos y en la Carta de Derechos Fundamentales de la UE… el elevado listón impuesto por el TJUE a la hora de señalar los criterios que deberían ser tenidos en cuenta a la hora de regular un sistema de conservación preventiva de datos relativos a las comunicaciones electrónicas de los usuarios de tales servicios (v. gr., un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave) dificulta enormemente el surgimiento de una normativa, nacional o europea, compatible con la interpretación de la Carta Europea que realiza el TJUE. A diferencia del «acceso» o cesión a las autoridades correspondientes, más maleable a la hora de ser sometido a específicos criterios subjetivos, objetivos, materiales y temporales que justifiquen la idoneidad, necesidad y proporcionalidad de la injerencia, la «conservación» resulta ser mucho más compleja de someterse a los parámetros indicados por el Tribunal de Luxemburgo (Ortiz-Pradillo, 2020, págs. 1-28).

Por su parte, Alfredo Gutiérrez Ortiz Mena (2014), reflexiona:

Uno de los temas más relevantes en las democracias constitucionales modernas es el que relaciona a los elementos del título de esta aportación: la esfera de libertades que se asocian a la intimidad o privacidad de las personas y el potencial de la tecnología comunicativa para develar aspectos importantes de la vida privada al conocimiento del público. La pregunta por la correcta relación de ambos no solo es de suma importancia para la resolución de asuntos prácticos y concretos en una diversidad de temas, sino también, en general, para la definición del modelo de Estado que estamos dispuestos a defender, y en particular, la forma de interpretar su expresión jurídica al reflejarse en determinadas normas constitucionales, …En casos futuros que involucren tecnología equivalente, estimo que los jueces constitucionales deberán analizar con igual visión integral la preocupación constitucional de proteger la intimidad de las personas, y habrá de analizarse nuevas posibilidades de abuso en el almacenamiento de datos que revelen aspectos de la identidad de las personas sobre los cuales podría existir una expectativa de privacidad legítima. Si este llegara a ser el caso, la expectativa de privacidad legítima habría, a diferencia de este caso, de ameritar una protección constitucional mayor, por tanto, la aplicación de un escrutinio estricto que no solo amerite verificar los pasos de la necesidad, idoneidad y proporcionalidad, sino también requiera de la participación de una autoridad judicial para su utilización. Sin embargo, este no es el caso que tenemos que resolver en este asunto, y forma parte de una discusión abierta (Gutiérrez Ortiz Mena, 2014, págs. 239-245).

En igual sentido, se adscriben William Guillermo Jiménez y Orlando Meneses Quintana (2023), cuando sostienen, que «existen derechos fundamentales que en ocasiones entran en conflicto en las comunicaciones de Internet y las redes sociales, medios tecnológicos caracterizados por el anonimato, la fácil reproducción y copia, la alta popularidad y el fácil acceso»

La Estrategia Nacional de Ciberseguridad de Paraguay 2024-2028

La Ley n.°4989/2013, «Que crea el marco de aplicación de las Tecnologías de la

Información y Comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)», establece en su art. 4: «… promover la seguridad informática y de redes para desarrollar las tecnologías de la información y comunicación» (BACCN, 2016).

La elaboración del Plan Nacional de Ciberseguridad por parte de la SENATICs, en coordinación con el Ministerio de Relaciones Exteriores −MRE− y con la participación de los diversos sectores involucrados, bajo el apoyo y facilitación de la Organización de los Estados Americanos −OEA−, presentado a través de la SENATICs por Nota n.° 49/17, de fecha 20 de marzo de 2017, es aprobado por el Decreto n.° 7052/2017 «Por el cual se aprueba el plan nacional de ciberseguridad y se integra la Comisión Nacional de Ciberseguridad» es consecuencia directa de la creación de la SENATICs y, desde luego, de la política nacional adoptada sobre ciberseguridad en Paraguay (base legal.com.py, s. f.).

Debe destacarse que el Plan Nacional de Ciberseguridad definía ya lo que debía de entenderse por delitos informáticos, y en tal sentido, sostenía: «actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta de delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito» (National Cyber Security Strategy, 2017, pág. 1).

La SENATICs evoluciona convirtiéndose en MITIC por Ley n.° 6207 de fecha 22 de octubre del 2018 (BACCN, 2019).

En efecto, el referido plan define lo siguiente:

> "Plan Nacional de Ciberseguridad, producto de un trabajo multi-stakeholder de varios años, y de un proceso que involucró representantes de más de 120 organizaciones, entre ellas instituciones públicas, sector privado, academia, sociedad civil, gremios profesionales y organismos internacionales, entre otros, ...Este camino recorrido condujo a la inclusión de la Ciberseguridad y la protección de la información como un eje misional del MITIC, a través de una Dirección General de Ciberseguridad y Protección de la Información, con atribuciones y un organigrama acorde a los desafíos a los que se enfrente" (MITIC, s. f., pág. 1).

Actualmente, el Ministerio de Tecnologías de la Información y Comunicación, MITIC, con ayuda del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo −CICTE− de la Organización de Estados Americanos −OEA−, a través del Centro de respuestas ante incidentes cibernéticos CERT-Py, trabaja en la actualización de aquel Plan Nacional, que, hoy denomina, Estrategia Nacional de Ciberseguridad de Paraguay 2024-2028, que lanzó el pasado 7 de junio del año en curso (CERT-Py, s. f.) y con ella se materializarán las decisiones de política pública en materia de ciberseguridad en el Paraguay en los próximos cuatro años.

El Gobierno Nacional hoy habla de una agenda digital, de Gobierno digital. Es en este escenario que se construye la señalada estrategia nacional.

> Se prevé que el proceso culmine en diciembre de 2024. Con las informaciones recabadas en las mesas de diálogo, lanzamiento y mesa técnicas, próximamente, se elevará a consulta pública un borrador de la estrategia. Además, se prevé un plan de implementación que incluya responsables y posibles fuentes de financiamientos (CERT-Py, s. f.).

El Departamento de Cibercrimen y Lucha contra los Delitos Informáticos de la Policía Nacional

La Ley n.° 5757/2016 que modifica varios arts. de la Ley n.° 222/1993 Orgánica de la Policía Nacional, en su art. 166 establece la dirección general de Investigación Criminal que conforme a su art. 171 está integrada por una dirección de Investigación de Hechos Punibles Económicos y Financieros y ésta a su vez por el Departamento Especializado en la Investigación del Cybercrímen y los Hechos Punibles Informáticos.

Dicho departamento recibe permanentemente denuncias sobre fuga de datos de dispositivos móviles, especialmente relacionada a imágenes personales de sus propietarios (ABC, Nacionales, 2023).

La Unidad Especializada de Delitos Informáticos del Ministerio Público

La Unidad Especializada de Delitos Informáticos de Ministerio Público fue creada, según se expresa en su propia página web, para, «combatir los hechos punibles cometidos a través del uso de la tecnología que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital» (Ministerio Público, 2024).

> Según las Resoluciones n.° 3459/10 y n.° 4408/11, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos son los siguientes: Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos (Ministerio Público, 2024, pág. 1).

A lo que debe sumarse el asesoramiento a los agentes fiscales en el registro, secuestro, operaciones técnicas y procedimientos procesales relacionados a los delitos informáticos.

Resulta interesante la definición de delitos informáticos que se encuentra en la página web del Ministerio Público, donde se lee que estos son, «todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas» (Ministerio Público, 2024, pág. 1).

Sin embargo, junto con las denuncias relacionadas con las falsificaciones de tarjetas, el acceso indebido a sistemas informáticos, la gran cantidad de denuncias relacionadas con la pornografía infantil, la cual según una publicación de ABC, en el 2021 alcanzó la cantidad de 2600 y la realización del operativo: luz de infancia, para desarticular una red internacional de pornografía infantil (ABC, Nacionales, 2022), no es un dato menor y de hecho invita a cuestionarse los límites de la definición de delitos informáticos sostenida por el Ministerio Público en su página web.

La evidencia digital en el convenio de Budapest

Ley nacional que aprueba el convenio de Budapest

La Ley n.° 5994, del 26 de julio del 2017, Que aprueba la convención sobre la ciberdelincuencia, y el protocolo adicional al convenio sobre ciberdelincuencia relativo a la

penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (BACCN, 2021).

Por esta ley, finalmente, el Paraguay incorpora a su legislación positiva una serie de definiciones, tales como, lo que debe entenderse por: sistemas informáticos, datos informáticos, proveedor de servicios y datos relativos al tráfico, establece igualmente tipificaciones delictivas y recomendaciones procesales (Rojas Benítez, 2020).

Con este convenio, instrumento jurídico adoptado por el Paraguay, bien se pueden:

> …castigar los hechos punibles realizados en el extranjero por entender con el artículo 8.8 de nuestro Código penal, que se está ante bienes jurídicos de protección universal, bajo las reglas, claro, tanto del Código penal como las del propio convenio, en la persecución y castigo de los señalados hechos punibles (Rojas Benítez, 2020, pág. 165).

Conservación, registro, confiscación, obtención en tiempo real de datos de tráfico y la obligación de mantener en secreto estos procedimientos

¿Qué es tráfico de datos o datos de tráfico según el Convenio de Budapest? Resulta pertinente apuntar que el art. 1. d) del Convenio de Budapest, define, datos de tráfico y, en tal sentido, establece que son:

> …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 (OAS, 2001, pág. 2).

El Convenio de Budapest sancionado por Ley n.° 5994, del 26 de julio del 2017, en cuatro títulos y cinco artículos establece todo un sistema para la conservación rápida de datos por un plazo de 90 días renovables, la obligación de presentarlos a las autoridades competentes ya sea por parte de una persona o proveedor de servicio que comunique datos que obren en su poder, estos deberán incluso proveer datos relativos a los abonados, es decir, cualquier información que se refiera a los abonados de un servicio diferente de los datos de tráfico (OAS, 2001).

Por el mismo convenio se faculta a las autoridades al registro y confiscación de datos informáticos de sistemas informáticos específicos o similares a los primeros. Se regula la obtención en tiempo real de datos informáticos y entiéndase con esto la posibilidad de grabar en tiempo real estos datos de tráfico de comunicaciones específicas transmitidas en el territorio paraguayo. De igual manera, fuera de los tipos penales que el Convenio de Budapest establece en sus art. 2 al 12, este deja abierta la posibilidad de interceptar datos de tráfico relativos a otros delitos graves que deberán, ser definidos.

En todos los supuestos, estos datos pueden ser obtenidos ya sea de una persona o de un proveedor de servicios e igualmente, en todos estos supuestos el convenio prevé la posibilidad de ordenar a estos mantener en secreto la ejecución de dichos procedimientos (OAS, 2001).

En tal sentido, se expresan: el Título 2, Conservación rápida de datos informáticos almacenados, bajo sus arts. 16 y 17; el Título 3, Orden de prestación, bajo su art. 18; el Título 4, Registro y confiscación de datos informáticos almacenados, bajo su art. 19; el Título 5, Obtención en tiempo real de datos informáticos, bajo sus art. 20 y 21.

En todos estos supuestos el propio convenio, ordena el respeto y protección de los derechos humanos y libertades fundamentales, establecidos en su artículo 15.

Segundo Protocolo adicional al Convenio sobre Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas

En Estrasburgo, el 12 de mayo del 2022, se concreta este segundo protocolo adicional (Eur-lex, 2023), con la intención de reforzar la cooperación internacional en materia de ciberdelincuencia. Este segundo protocolo hace hincapié en los proveedores de servicios en jurisdicciones extranjeras, trata de despejar las dificultades procesales que significa que la prueba o evidencia digitales se encuentre fuera de la jurisdicción europea.

La propia página web oficial de la Unión Europea, explica, sus características, retos y lo que pretende reforzar este segundo protocolo y lo hace en estos términos, aclarando que el mismo aún no se encuentra vigente:

Este Protocolo pretende reforzar aún más la cooperación internacional. Aborda el reto particular de las pruebas electrónicas relativas a la ciberdelincuencia y a otros delitos que son cometidos por los proveedores de servicios en jurisdicciones extranjeras, pero con poderes coercitivos restringidos a los límites nacionales. Sus principales características son:

- una nueva base jurídica que permita solicitar directamente a los registrantes de otras jurisdicciones obtener información sobre el registro de nombres de dominio;
- una nueva base jurídica que permite obtener información sobre los abonados directamente de los proveedores de servicios en otras jurisdicciones;
- medios mejorados para obtener información sobre los abonados y datos de tráfico a través de la cooperación entre Gobiernos;
- una cooperación acelerada en situaciones de emergencia, incluido el uso de equipos conjuntos de investigación e investigaciones conjuntas" (Eur-lex, 2023).

Reflexiones doctrinarias españolas en torno a la evidencia digital más allá de sus fronteras: en territorio europeo

Federico Bueno de Mata (2024), explica que:

> …con anterioridad, a través de la aplicación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, todos los Estados deberían trasponer la Orden Europea de Investigación en materia penal antes de mayo de 2017 como medio para luchar contra la criminalidad transfronteriza en el ámbito de la UE. En este sentido se pudo constatar que dicha orden nacía obsoleta y que la misma debía ser complementada con otros instrumentos: un reglamento que introduce las órdenes europeas para la obtención, la producción y el aseguramiento de pruebas electrónicas y una directiva sobre las obligaciones de los servidores que traten datos de ciudadanos europeos con las autoridades judiciales y policiales europeas. Dichas medidas fueron propuestas por la Comisión, a través de un comunicado de 17 de abril de 2018, pero debido al Covid-19 se postergó su aplicación y se retomó su tramitación cinco años más tarde con algunos cambios en la técnica legislativa (Bueno de Mata, 2024, págs. 305-307).

En esos términos explica, la actual existencia de un Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (Unión Europea, 2023).

En efecto de una Directiva −UE− 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales (Unión Europea, 2023).

Y en tal sentido, agrega Bueno de Mata (2024):

> La directiva establece normas para la representación legal de ciertos proveedores de servicios en la Unión Europea, con el fin de obtener pruebas en procesos penales, al tiempo que define obligaciones para estos proveedores, como recibir órdenes judiciales, Proporcionar datos necesarios, conservar información y enfrentar sanciones por incumplimiento. En este sentido, los Estados miembros deben asegurar que los proveedores designen representantes legales y proporcionen sus datos de contacto, con especificaciones sobre el idioma de las comunicaciones. En el otro lado, se establecen sanciones para el incumplimiento y un mecanismo de coordinación entre Estados miembros para que esta norma se convierta en realidad. A nivel temporal, la transposición de la directiva debe ocurrir en 30 meses desde su entrada en vigor, por lo que tendremos que esperar hasta 2026 para comprobar que estos instrumentos legislativos se convierten en derecho vigente (Bueno de Mata, 2024, págs. 305-307).

En este orden de ideas, Juan Antonio Muriel Diéguez (2024),

> …permitir ir a las autoridades de un Estado miembro obligar a empresas y/o entidades privadas la conservación o entrega de datos informáticos, aunque se hallen fuera de la jurisdicción de la UE. Es decir, podemos poner en duda la legalidad de ampliar el ámbito de actuación de este Reglamento a terceros fuera de la Unión Europea" (Muriel Diéguez, 2024), por otro lado, existen dudas sobre la proporcionalidad de la medida, por considerar que se pudiera dejar en indefensión al acusado (Muriel Diéguez, 2024, págs. 172-201).

La evidencia digital desde las normas del procedimiento penal paraguayo

En la segunda decena del siglo XXI es impensable que una persona no se encuentre conectada a un servidor de internet por algún tipo de dispositivo móvil en forma permanente, teléfonos, pulsera o anillos inteligentes, tabletas, computadoras, auriculares inalámbricos de traducción instantánea, libros electrónicos, la utilización cotidiana de GPS para posicionarnos y localizar, lo que fuere. Escuchamos música en línea, vemos películas en línea, nos ejercitamos y controlamos esto mismo en línea, compramos en línea, recibimos y damos clases en línea. Se es testigo, al decir de Henning Meyer (2017)«la robotización de la mayoría de los trabajos»(Meyer, 2016-2017, págs. 50-56). Se puede decir que el siglo XXI es sinónimo de una verdadera revolución digital (Cordon, Alons, & Martin, 2010).

A lo que debe sumarse la imperdible nueva actividad social, denominada, redes sociales. Todo se encuentra en línea y digitalizado. El formato papel de apoco va quedando en desuso. El vertiginoso cambio que inicia a finales del siglo XX con el uso de computadoras se transformó en una época casi absolutamente digitalizada y sigue avanzando hacia ese destino (Buckland, Garmilla, Murillo, & Silva-Flores, 2018). El tratado de Budapest es el resultado lógico de la necesidad de reglar dichos cambios ya desde principios del siglo XXI. Esta realidad, a su vez, transforma el escenario delictivo (OAS, 2001).

Al respecto, Montserrat De Hoyos Sancho (2023), sostiene con mucho acierto, que:

> …para investigar y probar un simple homicidio con arma blanca puede ser necesario obtener pruebas digitales del tipo: correos electrónicos entre autor y víctima, consulta de sus perfiles privados de Facebook o Instagram, mensajes de WhatsApp, compras online, coordinadas de GPS de una ruta determinada, rastreo de información buscada en internet, etc. Además, esas mismas fuentes nos indican que en dos tercios de estas investigaciones tales pruebas tuvieron que obtenerse de proveedores de servicios on line implantados en territorios de otras jurisdicciones. Por lo tanto, está claro que es imprescindible disponer de instrumentos normativos que permitan a las autoridades competentes obtener esa información electrónica tan necesaria, de manera selectiva, rápida y fiable, al tiempo que se asegura el pleno respeto de los derechos esenciales, que desde luego incluyen las garantías procesales fundamentales, así como la protección de la información y los datos personales (De Hoyos Sancho, 2023, págs. 99-128).

Por su parte, Javier Alonso Lecuit (2021), explica que:

> Los grandes proveedores de Internet, cuyo poder de mercado se apalanca en una ingente base de usuarios, marcan el ritmo de la transformación tecnológica de la red y las reglas de uso mundiales de las aplicaciones. En el plano técnico, algunas características (cifrado, arquitecturas de información virtualizadas y distribuidas, etc.) dificultan o en ocasiones impiden el curso de las investigaciones criminales. El encaje de este escenario con los diversos marcos legales nacionales y regionales plantea serias dificultades en la lucha internacional contra un número creciente de delitos que utilizan el ámbito digital para su consecución. Los medios técnicos y legislativos y las capacidades con que cuentan los cuerpos policiales y operadores judiciales requieren de una continua adaptación pareja al rápido proceso de digitalización de la sociedad (Alonso Lecuit, 2021, págs. 1-11).

En igual línea de consideraciones expresa Luis Gómez Amigo (2019) que, incluso señala la necesidad de contar con una prueba penal transfronteriza, explicando:

> De manera especial a partir de los atentados terroristas de París de noviembre de 2015 y Bruselas de marzo de 2016, la Unión Europea ha establecido como una de sus prioridades esenciales en materia penal facilitar la obtención de pruebas electrónicas de carácter transfronterizo, esenciales para poder investigar, y así evitar y perseguir de manera eficaz los delitos graves, en especial, los atentados terroristas. Téngase en cuenta, además, que a menudo las redes sociales y los servicios de correo electrónico y de mensajería instantánea son el único lugar donde los investigadores pueden hallar pistas para investigar el delito y pruebas para enjuiciarlo" (Gómez Amigo, 2019, págs. 23-56).

Asimismo, Carmen Cuadrado Salinas (2023), sostiene que:

> La finalidad de fomentar y facilitar una mayor y más eficiente cooperación con los proveedores de servicios se dirigía a posibilitar, no solo la obtención, sino también el aseguramiento, a través de una orden de conservación, de quienes tuviesen la posesión de cualquier dato electrónico que las autoridades investigadoras necesitasen (Cuadrado Salinas, 2023, págs. 117-135).

En la página del Ministerio Público, se puede leer que la unidad especializada de delitos informáticos presta colaboración y asesoramiento cuando de los procedimientos establecidos en los arts. 183, 192, 193 y 196 del CPP, se trata (Ministerio Público, 2024).

Igualmente, en la revista web de Acciones y Logros 2023 del Ministerio Público de la República del Paraguay, en la parte pertinente a esta unidad especializada, se puede leer que sólo en el año 2023 ingresaron 1.326 causas y que se han obtenido condenas elevadas. No obstante, lo anterior, también se puede leer que están trabajando con las NNUU para la producción de un manual de litigación y juicio oral (Ministerio Público, Acciones y Logros, 2023).

Al respecto, Federico Bueno de Mata (2023), sostiene:

> la prueba electrónica se convierte en una pieza de convicción fundamental en la investigación y el enjuiciamiento de delitos, siendo necesaria en un 85 % de las investigaciones penales, incluso cuando el delito no es informático. Unido a lo anterior, el legislador es consciente de que la Orden Europea de Investigación debe ser reforzada a través de mecanismos complementarios que recojan las particularidades de la comisión de delitos en Internet encaminados a obtener pruebas electrónicas por las distintas autoridades…en muchas ocasiones los procesos penales se suspenden e interrumpen porque los operadores de telecomunicaciones no contestan a las peticiones judiciales o se busca de manera intencionada que la información resida en servidores extranjeros de difícil acceso, con lo que se da una especie de «huida de la jurisdicción», lo que complica la investigación y el enjuiciamiento de determinados ciberdelitos" (Bueno de Mata, 2024, págs. 305-307).

El proyecto de ley para disponer la obligatoriedad de la conservación de datos de tráfico en los hechos punibles de pornografía infantil y hechos punibles conexos

Este proyecto de ley presentado por el diputado Rodrigo Blanco sigue en trámite desde el año 2022. La última vez, el pasado 24 de septiembre del 2024, fue nuevamente postergado su estudio por 15 días en la Cámara de Diputados (Silpy, 2024).

Este anteproyecto de ley que pretende la conservación obligatoria de datos de tráfico de internet por el lapso máximo de 1 año, para el hecho punible de pornografía infantil y hechos punibles conexos, posee 12 art. y se fundamenta básicamente en la necesidad de que el Ministerio Público cuente con la posibilidad de trazar los datos generado en internet y utilizados a través de ella con la ayuda de los prestadores de este servicio.

En su art. 6 este proyecto aborda la conservación de los datos, en los siguientes términos:

> En el marco del objeto de la presente Ley, los proveedores de servicios de acceso de internet y trasmisión de datos deberán conservar los datos de tráfico de las comunicaciones

por un período mínimo de 12 (doce) meses, en los términos establecidos en este artículo. Para el cumplimiento de lo dispuesto en este artículo, los datos serán almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información. Los proveedores de servicios de acceso de internet y trasmisión de datos deberán almacenar sólo aquellos datos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio (Silpy, 2024).

La autoridad de aplicación sería la CONATEL quien se encargaría de controlar y coordinar, verificar y dictar instrumentos administrativos para la conservación de datos de tráfico de internet y la identificación de usuarios, esto de conformidad a su art. 7.

Igualmente, la ley prevé sanciones pecuniarias de hasta mil jornales mínimos por el incumplimiento de las obligaciones establecidas en la misma. En tal sentido, debe apuntarse, que todas las personas, físicas o jurídicas, prestadoras de servicios de internet, son sujetos obligados a proporcionar la información requerida por el Ministerio Público y ordenada por el juez competente en causas de pornografía infantil o hechos punibles conexos a estos. Información que deberá ser proporcionada dentro de las 72 horas de recibida la orden del juzgado. La información consistirá en la identificación del protocolo de Internet IP del usuario (Silpy, 2024).

Método

Esta investigación analiza la evidencia digital y el proceso penal paraguayo a partir de la adhesión del Estado paraguayo al Convenio de Budapest y en tal sentido, se utiliza un enfoque cualitativo de diseño no experimental y de tipo documental.

En ese orden de ideas, como técnica de recolección de datos se aplicó análisis documental a través de la doctrina vinculante al tema, de las normas paraguayas y del mencionado convenio. El alcance de la investigación fue descriptivo (Courtis, 2006), (Sánchez Zorrilla, 2011), (Nizama Valladolid & Nizama Chávez, 2020).

Resultado y análisis

Límites constitucionales

El límite entre, la garantía del respeto a la vida privada que no afecte el orden público o derecho de terceros y la exigencia de una orden judicial, para los casos especialmente previstos en la ley, donde se permita registrar, reproducir, interceptar o secuestrar documentos o comunicación privada, junto con el derecho de toda persona a ser protegida en su libertad y seguridad, se encuentra difuso.

La gran pregunta es ¿se desdibujan estas garantías consagradas en los arts. 33, 36 y 9 de la norma constitucional al permitirse por ley procedimientos de captación de datos de tráfico en tiempo real en el territorio de la República del Paraguay? ¿Ante la posibilidad de almacenar datos de tráfico por 90 días y los datos de los abonados?

La necesidad de orden judicial para estos casos es desde luego incuestionable y legitimarán la incorporación válida al proceso penal de la evidencia digital obtenida en violación de tales garantías con rango constitucional.

No obstante, almacenar datos de tráfico por 90 días que podrán ser renovados, deja en entredicho la garantía del art. 33 que consagra el respeto a la vida privada cuando no afecte el orden público. Esto más bien parece una carta blanca al monitoreo y almacenamiento permanente de datos de tráfico, para la eventual revisión,o registro o secuestro de esta información en el marco de un procedimiento penal.

Este almacenamiento de datos de tráfico o si se prefiere su disponibilidad por el lapso de 3 meses renovables, debería mover a la Corte Suprema de Justicia como garante de la debida interpretación de las normas constitucionales, a pronunciarse al respecto de este versus entre los art. 33, 36 y 9 de la norma fundamental.

La evolución favorable de políticas sobre ciberseguridad en el Paraguay

Sin dudas la política pública paraguaya del siglo XXI se adecua a la arrolladora revolución digital, esto no podría ser de otra manera. En este contexto es que en la agenda estatal se habla de digitalización del país, en un gobierno digital,a través de expedientes electrónicos y hasta de una identidad digital para cada uno de sus habitantes.

En este contexto, en los últimos diez años en el Paraguay se habla de un plan nacional de ciberseguridad y se crea una Secretaria Nacional de Tecnologías de la Información y la comunicación −SENATICs−, y, se aprueba el Plan Nacional de Ciberseguridad y se integra una Comisión Nacional de Ciberseguridad. Esta secretaría evoluciona, por Ley n.° 6207/17, y se convierte en un ministerio: el Ministerio de Tecnologías de la Información y Comunicación, encargándose de la ciberseguridad y protección de la información del Estado y todos sus habitantes.

Toda esta política pública, bien encaminada, se encuentra actualmente en un proceso de revisión y fortalecimiento siempre en atención a las nuevas tecnologías que no desaceleran su crecimiento, lo que es absolutamente pertinente y deja ver el compromiso y a la vez los desafíos que el Paraguay asume en esta imparable evolución tecnológica, que, se traduce en un nuevo escenario delictivo: el cibercrimen o la ciberdelincuencia, como amenazas que necesitan de la *última ratio* del derecho penal y de acuerdos internacionales para combatirla adecuadamente.

En este contexto no es un dato menor el concepto de delitos informáticos que ya el Plan Nacional de Ciberseguridad sostenía, como: «actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta de delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito» (MITIC, s. f., pág. 1).

La amplitud de este concepto, entiendo, no puede dejar dudas en la investigación delictiva y en la actuación de la Policía Nacional, que hoy cuenta con un departamento de cibercrimen y lucha contra los delitos informáticos, dependiente de la dirección de Hechos Punibles Económicos y Financieros, dependiente a su vez de la dirección general de Investigación Criminal.

Si bien la definición puede mejorarse, la idea clara de que ya sea a través de la red informática mundial llamada internet, o bien a partir de los datos de tráfico que circulan por dicha red, se podrían cometer hechos punibles. De hecho, ambas aristas, son difícilmente desvinculables una de otra.

La una será siempre el medio necesario para que la otra aparezca. Luego, hablar de delitos cometidos a través de internet es hablar de delitos que obtienen o manipulan los datos de tráfico que en ella circulan, fuera de lo permitido por ley.

Por tanto, en la red o a través de la red de internet es lo mismo. Y en tal sentido, cuando en la Unidad Especializada de Delitos Informáticos del Ministerio Público, es creada para: «combatir los hechos punibles cometidos a través del uso de la tecnología que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital» (Ministerio Público, 2024, pág. 1).

Esta unidad especializada necesariamente deberá manejarse trasversal y conjuntamente con las demás unidades de trabajo del Ministerio Público, en atención justamente a la creciente diversidad de hechos punibles cometidos desde o a través de la red informática mundial llamada, internet.

La necesidad político criminal de controlar un difícil ámbito delictivo

La red internet y los datos de tráfico que en ella circulan, gracias a los proveedores y a los abonados del servicio, crean un escenario o una realidad muy singular en la que pueden originarse hechos delictivos de los más variados. Y al decir de los más variados, no se refiere exclusivamente a un acceso ilícito, interceptación de datos de tráfico, o a ataques a estos datos o a los sistemas informáticos en sí mismos, o a programas informáticos concebidos para delinquir, falsificaciones, fraudes, pornografía infantil o hechos punibles relacionados con la propiedad industrial o de marcas, que podríamos decir, son los más comunes. Sino más bien a que a través de la red de internet se puede, por ejemplo, realizar una coacción, una extorsión, amenazas de hechos punibles graves, falsificaciones de documentos, incluso lavar dinero, así como una vía para el terrorismo o su apología, y, por tanto, investigar y sancionar tal variedad de posibilidades delictivas, torna el escenario delictivo difícil de manejar.

La necesidad político criminal de controlar este ámbito delictivo, que no se cansa de innovar, es absoluta. A lo dicho debe sumarse, el principio de territorialidad de la jurisdicción para juzgar hechos punibles y la extraterritorialidad del tráfico de datos en la red de internet, y, con ello se genera impotencia.

En este contexto surge el Convenio de Budapest que ya en el 2004, entra en vigencia señalando en el escenario delictivo nuevos tipos penales y a su vez nuevos procedimientos para conservar, registrar, confiscar, obtener en tiempo real datos de tráfico e incluso expresa la obligación de mantener en secreto estos procedimientos penales.

Ahora bien, estos procedimientos encuentran su límite en el principio de territorialidad del procedimiento penal y, por tanto, esto mismo deja maniatados a los jueces que necesitan datos de tráfico que se encuentran en servidores fuera de su país, de manera que, torna inaplicable, en muchos casos, estos mecanismos procesales puestos en escena con dicho convenio.

Y ¿qué sucede con las filtraciones de información realizada por los propios proveedores del servicio de internet o de redes sociales como Facebook, Instagram, entre otras o servicios vinculados a posicionamientos geográficos, cuentas bancarias y datos aún más personales, como Uber, por ejemplo?

La comunidad europea recurrió a directivas y reglamentos que facultan al juzgador a solicitar datos de tráfico a proveedores del servicio de internet fuera del territorio de su país y dentro de la unión europea, pero, a su vez, se encuentran con que algunos proveedores de la red del servicio se encuentran en jurisdicciones extranjeras, es decir, fuera de la unión europea y esto dificulta, la evidencia digital en un proceso penal jurisdiccional.

En este contexto surge, el segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas, dado en Estrasburgo en el año 2022 y que se conoce coloquialmente como el segundo protocolo de Budapest. Este convenio aún no está en vigencia y el Paraguay no lo ha ratificado. El contenido de su normativa debe leerse a partir del señalado escenario delictivo descrito líneas arriba, para comprender el diseño internacional para combatir el cibercrimen que integra el procedimiento penal paraguayo.

El Código Penal Paraguayo, si bien en sus arts.7 y 8 cuenta con reglas de extraterritorialidad de los hechos perseguibles por jueces paraguayos, estos se limitan a las condiciones allí expuestas y dejando fuera otras, que tal vez con leyes puntuales se pudieran salvar o bien suscribiendo el segundo protocolo mencionado. Ahora bien, debe señalarse el riesgo de una jurisdicción internacional tal y como lo plantea este segundo protocolo, pero, este análisis ameritaría una investigación exclusiva respecto al tema.

Con la adopción del Convenio de Budapest a través de la Ley n.° 5994/2017 el sistema penal se adecua al diseño internacional o si se prefiere el procedimiento penal ahí establecido para combatir el cibercrimen en el Paraguay.

Es decir, procesalmente hablando, mediando orden judicial, en un proceso penal se puede: conservar, registrar, confiscar, obtener en tiempo real datos de tráfico e incluso se tiene la posibilidad legal de obligar a mantener en secreto estos procedimientos penales a los proveedores de servicios y las personas involucradas en los mismos.

En este orden de consideraciones, el proyecto de ley, «Que dispone la obligatoriedad de la conservación de datos de tráfico para combatir la pornografía infantil y hechos punibles conexos», resulta inoficiosa.

Conclusión

Se cuenta con un procedimiento penal para la obtención, registro, confiscación e incluso obtención de datos de tráfico en tiempo real e incluso la posibilidad legal para mantener este procedimiento en secreto, desde que se adoptó el Convenio de Budapest. Luego, hasta qué punto todo esto desdibuja las garantías y libertades constitucionales previstas en la norma fundamental, esta es aún tarea pendiente de la Sala Constitucional de la Corte Suprema de Justicia.

El Paraguay está invitado a adoptar el segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas, sin embargo, su adopción necesita una mayor discusión en el campo de la política criminal y del derecho internacional público en relación a la extraterritorialidad de la jurisdicción penal que este segundo protocolo conlleva.

Referencias

ABC. (21 de agosto de 2022). Nacionales. Pornografía infantil: en 2021 la Fiscalía más de 2.600 denuncias, págs. https://www.abc.com.py/nacionales/2022/08/21/pornografia-infantil-en-2021-la-fiscalia-recibio-mas-de-2600-denuncias/.

ABC. (2 de Marzo de 2023). Nacionales. Delitos informáticos: el 100% de las denuncias recibidas pertenecen a filtraciones y no a hackeo, págs. https://www.abc.com.py/nacionales/2023/03/02/delitos-informaticos-el-100-de-las-denuncias-recibidas-pertenecen-a-filtraciones-y-no-a-hackeo/. Recuperado el septiembre de 30 de 2024, de https://www.abc.com.py/nacionales/2023/03/02/delitos-informaticos-el-100-de-las-denuncias-recibidas-pertenecen-a-filtraciones-y-no-a-hackeo/

Alonso Lecuit, J. (2021). El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea . Real Instituto Elcano, 1-11.

BACCN. (25 de abril de 2016). Recuperado el septiembre de 29 de 2024, de https://www.bacn.gov.py/leyes-paraguayas/4766/crea-el-marco-de-aplicacion-de-las-tecnologias-de-la-informacion-y-comunicacion-en-el-sector-publico-y-crea-la-secretaria-nacional-de-tecnologias-de-la-informacion-y-comunicacion-senatics

BACCN. (25 de julio de 2019). Obtenido de https://www.bacn.gov.py/leyes-paraguayas/8933/ley-n-6207-crea-el-ministerio-de-tecnologias-de-la-informacion-y-comunicacion-y-establece-su-carta-organica

BACCN. (18 de noviembre de 2021). Obtenido de ttps://www.bacn.gov.py/leyes-paraguayas/9900/ley-n-5994-aprueba-la-convencion-sobre-la-ciberdelincuencia-y-el-protocolo-adicional-al-convenio-sobre-ciberdelincuencia-relativo-a-la-penalizacion-de-actos-de-indole-racista-y-xenofoba-cometidos-por-medio-de-s

baselegal.com.py. (s.f.). https://baselegal.com.py/. Recuperado el 29 de septiembre de 2024, de https://baselegal.com.py/docs/9e610686-bccc-11eb-8314-525400c761ca

Buckland, H., Garmilla, A., Murillo, D., & Silva-Flores, M. (2018). La revolución digital ante los grandes retos del mundo. 100 iniciativas de innovación social digital que están transformando América Latina. Barcelona: Esade. Instituto de innovación social.

Bueno de Mata, F. (2024). Crónicas de legislación procesal. Ars Iuris Salmanticensis, 305-307.
CERT-Py. (s.f.). www.cert.gov.py/. Recuperado el 29 de septiembre de 2024, de https://www.cert.gov.py/estrategia-nacional-de-ciberseguridad/

Cordon, J. A., Alons, J., & Martin, H. (2010). Los libros electrónicos: la tercera ola de la revolución digital. 13.

Courtis, C. (2006). Observar la ley : ensayos sobre metodología de la investigación jurídica. Alicante: Trotta.

Cuadrado Salinas, C. (2023). La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales ¿Nuevas perspectivas? IUS ET SCIENTIA, 117-135.

De Hoyos Sancho, M. (2023). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo. Revista de Estudios Europeos, (Extraordinario monográfico 1 (2023), 99-128.

Eur-lex. (28 de febrero de 2023). https://eur-lex.europa.eu/. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A22023A0228%2801%29

Eur-lex. (28 de noviembre de 2023). https://eur-lex.europa.eu/. Obtenido de https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-cybercrime.html

Gomez Amigo, L. (2019). Las órdenes europeas de entrega y conservación de pruebas penales electronicas: una regulación que se aproxima. Revista Española de Derecho Europeo 71, 23-56.

Gutiérrez Ortiz Mena, A. (2014). El derecho a la intimidad en la era de la tecnología de las comunicaciones: una reflexión desde el derecho constitucional. Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional, 239-245.

Intercontinental, E. (2000). Constitución de la República del Paraguay. Asunción: Intercontinental editora.

Jiménez, W.-G., & Meneses Quintana, O. (2023). Libertad de expresión en internet y redes sociales vs. derechos a la intimidad y el buen nombre. Prevalencia, colisión y ponderación en el Derecho constitucional (1992-2019). Revista Derecho del Estado , 275-304.

Meyer, H. (2016-2017). Comprender la revolución digital y lo que realmente implica. Anuario internacional cidob 2016-17, 50-56. Recuperado el 30 de septiembre de 2024, de file:///C:/Users/Olga%20Rojas%20Benitez/Downloads/330879-Texto%20del%20art%C3%ADculo-474673-1-10-20180110.pdf

Ministerio Público, R. d. (2023). Acciones y Logros. Asunción: Dirección de comunicación y prensa del Ministerio Público.

Ministerio Público, R. d. (30 de septiembre de 2024). Recuperado el 29 de septiembre de 2024, de https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-

MITIC. (s.f.). mitic.gov.py. (Ministerio de Tecnologías de la Información y Comunicación) Recuperado el 29 de septiembre de 2024, de https://mitic.gov.py/ciberseguridad-y-proteccion-de-la-informacion/

Muriel Diéguez, J. A. (2024). Las Órdenes de Entrega y Conservación de Pruebas Electrónicas en el Proceso Penal Europeo. Revista De Estudios Europeos, 83, 172-201.

National Cyber Security Strategy, P. 2. (2017). afyonluoglu.org. Recuperado el 29 de septiembre de 2024, de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://afyonluoglu.org/PublicWebFiles/strategies/America/Paraguay%202017%20National%20Cyber%20Security%20Strategy.pdf

Nizama Valladolid, M., & Nizama Chávez, L. M. (2020). El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis. Vox Juris, 69-90.

OAS. (23 de Noviembre de 2001). www.oas.org. Recuperado el septiembre de 30 de 2024, de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Oromí i Vall-llovera, S. (2020). Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE. Revista de los Estudios de Derecho y Ciencia Política, 1-13.

Ortiz-Pradillo, J. C. (2020). Europa: Auge y Caída de las Investigaciones Penales Basadas en la Conservación de Datos de Comunicaciones Electrónicas. Revista General de Derecho Procesal, 1-28.

Rojas Benítez, O. (2020). Aspectos dogmático-penales y político criminales de la cyber delincuencia en el Paraguay. Revista Jurídica Facultad de Ciencias Sociales y Jurídica UNIBE, 165-190.

Sánchez Zorrilla, M. (2011). La metodología en la investigación jurídica: características peculiares y pautas generales para investigar en el derecho. Revista Telemática de Filosofía del Derecho, 317-358.

Silpy, S. d. (septiembre de 24 de 2024). https://silpy.congreso.gov.py. Obtenido de https://silpy.congreso.gov.py/web/expediente/126831

Unión Europea, U. (28 de JULIO de 2023). https://www.boe.es/. Obtenido de https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81097

Unión Europea, U. (28 de julio de 2023). https://www.boe.es/. Obtenido de https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81098