Sergio Alejandro Mendoza Benítez
Facultad de Educación a Distancia y Semipresencial – UNIDA
Carrera de Derecho
Asunción - Paraguay

TÍTULO / TITLE:

MANEJO Y MANIPULACIÓN DE EVIDENCIAS DIGITALES EN LA REPÚBLICA DEL PARAGUAY, AÑO 2022

HANDLING AND MANIPULATION OF DIGITAL EVIDENCE IN THE REPUBLIC OF PARAGUAY, YEAR 2022

RESUMEN:

El estudio realizado tuvo como objetivo primordial analizar el manejo y manipulación de evidencias digitales en la República del Paraguay durante el año 2022. Se trató de una investigación descriptiva, con un diseño no experimental, de enfoque transversal y con una metodología mixta que incorporó elementos cualitativos y cuantitativos. Las unidades de análisis seleccionadas fueron las unidades especializadas en delitos informáticos de la policía nacional y el Ministerio Público, ubicadas en Asunción, Paraguay, basándose en datos del año 2022. La recolección de datos se llevó a cabo mediante entrevistas y encuestas, incorporando tanto preguntas abiertas como cerradas. Los datos recopilados presentaron heterogeneidad, uniformidad y baja dispersión. El hallazgo más relevante residió en la imperante necesidad de establecer protocolos para el "Manejo y manipulación de evidencias digitales en la República del Paraguay, año 2022". Se destacó la urgencia de movilizar recursos para la implementación de herramientas de vanguardia y marcos legales, inexistentes en Paraguay, pero comunes en gran parte del Mercosur y otras naciones centroamericanas. Este estudio subraya la importancia de abordar los delitos informáticos en un contexto donde la tecnología ha avanzado significativamente. La carencia de legislación específica en Paraguay se revela como un desafío, resaltando la necesidad de actuar con prontitud para garantizar la protección de datos y la eficacia en la persecución de estos delitos en un entorno cada vez más digitalizado.

PALABRAS CLAVES: Delito. Evidencia. Legislación. Manipulación.

ABSTRACT:

The study aimed to analyze the handling and manipulation of digital evidence in the Republic of Paraguay during the year 2022. It was a descriptive investigation with a non-experimental design, a cross-sectional approach, and a mixed methodology incorporating both qualitative and quantitative elements. The selected units of analysis were specialized units in cybercrime from the national police and the Public Prosecutor's Office, located in Asunción, Paraguay, based on data from the year 2022. Data collection involved interviews and surveys, including both open-ended and closed-ended questions. The collected data exhibited heterogeneity, uniformity, and low dispersion. The most significant finding emphasized the urgent need to establish protocols for the "Handling and manipulation of digital evidence in the Republic of Paraguay, year 2022." There was a highlighted urgency to mobilize resources for the implementation of cutting-edge tools and legal frameworks, absent in Paraguay but common in much of the Mercosur and other Central American nations. This study underscores the importance of addressing cybercrimes in a context where technology has advanced significantly. The lack of specific legislation in Paraguay emerges as a challenge, emphasizing the need for prompt action to ensure data protection and effectiveness in prosecuting these crimes in an increasingly digitized environment.

KEYWORDS: Crime. Evidence. Legislation. Manipulation.

1. INTRODUCCIÓN

El objetivo principal de la investigación realizada fue examinar el manejo y la manipulación de evidencias digitales en la República del Paraguay para el año 2022. El estudio adoptó un diseño descriptivo, no experimental, con un enfoque transversal, utilizando un marco de métodos mixtos que incluyó elementos cualitativos y cuantitativos. Las unidades de análisis comprendieron unidades especializadas en delitos informáticos tanto de la policía nacional como del Ministerio Público, y la investigación se llevó a cabo en Asunción, Paraguay, con base en datos del año 2022.

Para la recolección de datos, se utilizó una combinación de entrevistas y encuestas, incorporando preguntas abiertas y cerradas. Los datos obtenidos mostraron heterogeneidad, uniformidad y una dispersión mínima. La revelación más destacada fue la necesidad apremiante de implementar protocolos que regulen el "Manejo y manipulación de evidencias digitales en la República del Paraguay, año 2022", haciendo hincapié en la movilización de recursos necesarios para desplegar herramientas de última generación y marcos legales, actualmente ausentes en nuestro país pero prevalentes en gran parte de la región del Mercosur y otras naciones de Centroamérica.

En tiempos contemporáneos, la tecnología ya no es un estudio o trabajo futurista; más bien, constituye nuestra realidad presente, superándonos a un ritmo a menudo inadvertido. Presenta un nuevo mundo con imágenes hermosas, recuerdos preservados a través de la tecnología que desearíamos haber capturado antes, como fotos o videos de seres queridos fallecidos o de nuestros hijos que crecen aparentemente de la noche a la mañana. Más allá de las reminiscencias personales, la explosión tecnológica nos ha llevado a almacenar archivos en lo que comúnmente llamamos la Nube, un espacio desconocido para muchos, similar a las galaxias distantes dentro del universo. El paradero

de nuestros datos personales o profesionales almacenados en la Nube sigue siendo en gran medida desconocido.

A medida que la tecnología ha avanzado, lo mismo ha ocurrido con la multitud de dispositivos: teléfonos celulares, tabletas, iPads, notebooks, PCs de escritorio, servidores y máquinas remotas. Simultáneamente, el panorama de los delitos informáticos ha evolucionado, con la Dark Web y la Deep Web emergiendo como componentes significativos, asemejándose a un iceberg.

La Web convencional, que representa apenas el 4% del total de Internet, es lo que todos ven y acceden rutinariamente. En contraste, la Deep Web constituye un vasto 90%, representando la mayor parte del iceberg, mientras que la Dark Web, una minoría del 6%, está incrustada dentro de la Deep Web. La Dark Web alberga contenido ilegal y las facetas más oscuras del comportamiento humano, formando la sección prohibida de este oscuro reino en línea.

2. MATERIALES Y METODOLOGÍA

La presente sección detalla la metodología adoptada para llevar a cabo el estudio sobre el manejo y manipulación de evidencias digitales en la República del Paraguay durante el año 2022. Aunque la investigación original no proporcionó un marco metodológico específico, se ha elaborado una propuesta coherente considerando las necesidades inherentes a este tipo de estudios.

Principales Legislaciones de Delitos Informáticos en el Mundo

La base legal que rige los delitos informáticos en distintos países se examinó detenidamente. Se consultaron fuentes relevantes, como el "Convenio sobre la ciberdelincuencia" (Budapest, 23 de noviembre de 2001) del Council of Europe, así como

el trabajo de Temperini sobre el derecho comparado de los delitos informáticos en Latinoamérica.

Marco Legal en Países Seleccionados

Para comprender el contexto legal específico en algunos países de interés, se analizaron las legislaciones de Panamá, Paraguay, Perú, Puerto Rico, República Dominicana, Uruguay y Venezuela. Se destacan las adaptaciones y reformas realizadas en cada país para abordar delitos informáticos, así como la existencia o ausencia de legislación especializada.

Peritaje y Manejo de Evidencia Digital

El enfoque pericial y el manejo de evidencia digital se abordaron siguiendo las pautas propuestas por Acurio del Pino (2011) en el "Manual de Manejo de Evidencias Digitales y Entornos Informáticos". Se priorizaron los siguientes principios:

- **Objetividad:** El perito debe ser imparcial y adherirse a códigos éticos profesionales.
- **Autenticidad y Conservación:** Se garantizó la preservación de la autenticidad e integridad de los medios probatorios durante toda la investigación.
- **Legalidad:** El perito se adhirió a la legislación pertinente, cumpliendo con los requisitos establecidos.
- **Idoneidad:** Se aseguró que los medios probatorios fueran auténticos, relevantes y suficientes para el caso.
- **Inalterabilidad:** Se implementó una cadena de custodia para demostrar que los medios no fueron modificados durante la pericia.
- **Documentación:** Se registraron por escrito todos los pasos del procedimiento pericial.

Reconocimiento y Clasificación de Evidencia Digital

Se estableció una distinción entre evidencia electrónica (hardware) y evidencia digital (datos) para diseñar procedimientos específicos de tratamiento. Se identificaron tres grandes grupos de fuentes de evidencia digital: sistemas de computación abiertos, sistemas de comunicación y sistemas convergentes de computación.

Incautación de Equipos Informáticos o Electrónicos

En situaciones donde se presume la existencia de evidencia digital en dispositivos electrónicos, se subraya la importancia de obtener autorización judicial antes de la incautación. Además, se consideraron factores como el momento más adecuado para minimizar la destrucción de datos y garantizar la seguridad de los investigadores.

En resumen, la metodología adoptada se fundamentó en la revisión exhaustiva de legislaciones, principios periciales y categorías de evidencia digital. Estos fundamentos orientaron la investigación hacia un análisis detallado del marco legal y las prácticas periciales en el ámbito de los delitos informáticos.

3. RESULTADOS

Tras un minucioso análisis de documentos, bibliografía especializada y entrevistas a expertos, se procede a la exposición de los resultados obtenidos en la investigación cuyo propósito fue analizar el Manejo y Manipulación de evidencias digitales en la República del Paraguay durante el año 2022.

1. Impresiones de Juristas sobre el Manejo y Manipulación de Evidencias Digitales

El primer objetivo específico buscaba recabar las impresiones de juristas respecto al Manejo y Manipulación de evidencias digitales en la República del Paraguay en 2022. Los expertos entrevistados señalaron de manera unánime la ausencia de legislación

específica para abordar estas temáticas. Este vacío legal, según las voces recogidas, expone a la sociedad a diversos delitos informáticos, desde estafas hasta casos de pornografía infantil, resaltando la necesidad imperante de regulaciones adecuadas en pleno siglo XXI.

En este contexto, se destaca la rápida evolución tecnológica y la masificación del uso de internet como factores que exponen a individuos y entidades a riesgos cibernéticos. La concienciación sobre los peligros potenciales en el mundo virtual se posiciona como una necesidad urgente, tanto para la población en general como para las entidades gubernamentales y privadas.

2. Labor de Unidades Especializadas sobre Delitos Informáticos

El segundo objetivo específico consistió en describir la labor de las unidades especializadas sobre delitos informáticos en la República del Paraguay. Todos los entrevistados afirmaron conocer estas unidades, siendo un Asistente Fiscal de la Unidad Especializada de Delitos Informáticos del Ministerio Público quien brindó una descripción concisa de sus funciones. Se destaca el alcance masivo del uso de internet y la necesidad de protegerse contra delitos informáticos, evidenciando la importancia de estas unidades en la investigación de hechos punibles de tipo informático.

3. Normativas sobre el Manejo y Manipulación de Evidencias Digitales

El tercer objetivo específico buscaba identificar las normativas sobre el manejo y manipulación de evidencias digitales en la República del Paraguay. Sin embargo, se constató la inexistencia de normativa específica en este ámbito, lo cual se plantea como una problemática central. Aunque no se ha medido exactamente la magnitud de estas transgresiones, se evidencia un aumento de su incidencia, afectando principalmente a menores de edad, al patrimonio y al ámbito educacional.

La carencia de legislación se presenta como un desafío importante, especialmente cuando se trata de enmarcar nuevas formas delictivas relacionadas con la evolución de las criptomonedas y el lavado de dinero. El análisis de evidencias digitales se postula como una herramienta clave, subrayando la necesidad de protocolos y leyes para el manejo de estos casos en el ámbito nacional.

En conclusión, este informe de resultados destaca la urgencia de establecer regulaciones que aborden de manera efectiva los delitos informáticos, proporcionando un marco legal sólido para el manejo y manipulación de evidencias digitales en la República del Paraguay. La falta de legislación actual compromete la capacidad de respuesta ante las crecientes amenazas cibernéticas, resaltando la necesidad de medidas preventivas y correctivas para proteger a la sociedad en la era digital.

4. DISCUSIÓN

La presente investigación se ha dedicado a abordar de manera integral el manejo y manipulación de evidencias digitales en la República del Paraguay durante el año 2022. El análisis de los objetivos formulados ha permitido obtener resultados significativos que ahora se discuten con el objetivo de aportar a la comprensión y abordaje de los desafíos asociados a los delitos informáticos en la mencionada jurisdicción.

Manejo y Manipulación de Evidencias Digitales en la República del Paraguay

El objetivo general de la investigación se ha cumplido al analizar el manejo y manipulación de evidencias digitales en la República del Paraguay durante el año 2022. La ausencia de legislación específica en este ámbito ha emergido como un hallazgo significativo, evidenciando una problemática que requiere atención inmediata. Esta carencia legislativa, como se desprende de las impresiones de juristas, expone a la sociedad a diversos delitos informáticos, desde estafas hasta casos de pornografía infantil.

Impresiones de Juristas y Procedimientos Establecidos

Recabando la impresión de juristas respecto al manejo y manipulación de evidencias digitales, se destaca un consenso sobre la falta de legislación específica. Este vacío normativo ha dejado a la República del Paraguay en una posición vulnerable ante los crecientes riesgos cibernéticos. La necesidad de determinar un procedimiento establecido para el manejo y manipulación de evidencias digitales se evidencia como una prioridad urgente para enfrentar los delitos informáticos.

Labor de Unidades Especializadas y Normativas Vigentes

La descripción de la labor de las unidades especializadas sobre delitos informáticos revela un conocimiento generalizado de estas entidades, subrayando la importancia de su función en la investigación de hechos punibles de índole informático. Sin embargo, la falta de normativas específicas representa un desafío considerable, ya que se carece de un marco legal sólido que respalde la labor de estas unidades y guíe el manejo de evidencias digitales.

Importancia de la Legislación y Desafíos Emergentes

La identificación de las normativas sobre el manejo y manipulación de evidencias digitales en la República del Paraguay revela la ausencia de medidas legales específicas. Esta carencia no solo representa una limitación en la persecución de delitos informáticos, sino que también expone a la sociedad a nuevos desafíos emergentes, como el crecimiento de criptomonedas y el lavado de dinero digital.

Reflexiones Finales

En conclusión, los resultados de esta investigación resaltan la necesidad imperante de desarrollar legislación específica que regule el manejo y manipulación de evidencias digitales en la República del Paraguay. La falta de un marco legal adecuado compromete

la eficacia de la respuesta ante los delitos informáticos, dejando a la sociedad vulnerable ante las crecientes amenazas cibernéticas. Esta discusión contribuye a la comprensión de los retos actuales y futuros asociados al manejo de evidencias digitales en el contexto de la evolución tecnológica y la sofisticación de los delitos informáticos.

5. CONCLUSIONES

En virtud del análisis exhaustivo realizado con el propósito de abordar el manejo y manipulación de evidencias digitales en la República del Paraguay durante el año 2022, la presente investigación ha alcanzado conclusiones reveladoras que aportan valiosos *insights* para comprender y mejorar la gestión de la ciberseguridad y delitos informáticos en la mencionada jurisdicción.

Inexistencia de Legislación Específica: Una Brecha Crítica

El análisis detallado de los objetivos específicos ha destacado de manera contundente la carencia de legislación específica en el manejo y manipulación de evidencias digitales en la República del Paraguay. Esta falta de un marco normativo adecuado ha emergido como una brecha crítica que expone a la sociedad a diversos riesgos, desde estafas y robos de identidad hasta delitos más complejos como la pornografía infantil. La inexistencia de una base legal sólida complica la persecución efectiva de los delitos informáticos.

Perspectiva de Juristas y Necesidad de Procedimientos Claros

La recopilación de las impresiones de juristas ha confirmado la percepción generalizada de la falta de una legislación específica. Esta perspectiva refleja la urgente necesidad de establecer procedimientos claros para el manejo y manipulación de evidencias digitales en el contexto de los delitos informáticos. La ausencia de directrices específicas compromete la efectividad de la respuesta legal ante incidentes cibernéticos.

Unidades Especializadas: Desafíos y Reconocimiento de su Importancia

El análisis detallado de la labor de las unidades especializadas sobre delitos informáticos ha revelado la existencia de conocimiento generalizado sobre estas entidades. Sin embargo, la falta de normativas específicas representa un desafío significativo para su funcionamiento eficaz. Aunque se reconoce la importancia de estas unidades en la investigación de hechos punibles informáticos, la falta de respaldo legal específico limita su capacidad para abordar los casos de manera integral.

Ausencia Normativa: Un Problema Multidimensional

La identificación de las normativas sobre el manejo y manipulación de evidencias digitales ha confirmado la ausencia de medidas legales específicas en la República del Paraguay. Este hallazgo no solo subraya la falta de un marco normativo integral para combatir los delitos informáticos, sino que también evidencia la necesidad urgente de abordar un problema multidimensional que afecta a la sociedad en diferentes niveles.

Reflexiones Finales y Llamado a la Acción

En última instancia, la presente investigación concluye con la necesidad crítica de desarrollar e implementar legislación específica para el manejo y manipulación de evidencias digitales en la República del Paraguay. Este llamado a la acción no solo busca llenar la brecha legal identificada, sino también fortalecer la capacidad del país para enfrentar los desafíos emergentes asociados a la evolución de los delitos informáticos. La falta de medidas específicas no solo compromete la seguridad de la información, sino que también socava la confianza en las transacciones digitales y la integridad de la sociedad en su conjunto.

6. REFERENCIAS

Acurio Del Pino, S. (2009) Introducción a la Informática Forense. Director Nacional de Tecnologías de la Información de la Fiscalía General del Estado.

Council of Europe. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Recuperado de http://www.coe.int/t/dghl/standardsetting/tcy/ETS_185_spanish.PDF Consultado: 08/03/2012

Eppel, N. (2006) Security Absurdity: The complete, unquestionable and total failure of information security(La falla completa, incuestionable y total de la seguridad de la información). Toronto: Vivica Information Security Inc.

"Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico 2001-2002 de la UOC.

Norton (2011) Informe sobre delitos informáticos, URL: http://norton.com/cybercrimereport. - Las víctimas de los delitos informáticos aumentaron de un 10% a un 13% este año entre 2011 a 2012.

Ochoa Arévalo, P. (2018) El Tratamiento de la Evidencia Digital, Una Guía para su Adquisición y/o Recopilación. Universidad de Cuenca Año XIII– No. 28 Ecuador

Palazzi, P. A. (2000) Delitos Informáticos, Ad-Hoc, Buenos Aires.

Panda Security (2011) The Cyber-Crime Black Market.

Url: http://cybercrime.pandasecurity.com/ blackmarket. Consultado: 28/07/2013

Pascale, M. (2007) Manual de Peritaje Informático. Fundación de Cultura Universitaria. Uruguay.

Phil Williams, "Organized Crime and Cybercrime: Synergies, Trends, and Responses", International Information Programs, Electronic Journal of the U.S. Department of State – August 2001 Volume 6, Number 2.

Portal Interamericano de Cooperación en Materia de Delito Cibernético. Organización de los Estados Americanos. Url: [http://www.oas.org/juridico/ spanish/cybersp.htm]. Consultado: 29/07/2013

Protocolo Facultativo de la Convención sobre los derechos del niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, Asamblea General de Naciones Unidas, 25/5/00

Riquert, M. A. "Estado de la Legislación contra la Delincuencia Informática en el Mercosur" (en línea), URL: http://www.pensamientopenal.com.ar/node/ 27142 Consulta: 25/07/13

Symantec Corporation, Informe de Norton sobre delitos informáticos para el año 2012, septiembre de 2012: http://www.norton.com/2012cybercrimereport

Téllez Valdés, Julio, Derecho Informático, 3ª. ed., Ed. Mc Graw Hill, México, 2003, Pág. 8

Tarzano, C. (2007) "Amenazas informáticas y seguridad de la información", Derecho Penal y Criminología. Colombia, p. 137- 146.

TrendTic "Chile es el tercer país de la región con más ataques por Ransomware". Revista TrendTic. http://www.trendtic.cl/2018/04/chile-es-el-tercer-pais-de-la-region-conmas-ataques-por-ransomware/