UNIVERSIDAD SIGLO XXI

VICERRECTORADO DE INNOVACIÓN, INVESTIGACIÓN
Y POSGRADO
MAESTRÍA EN DERECHO PROCESAL

ESTAFA INFORMÁTICA: EL CASO DE LA INCORPORACIÓN DE LA PRUEBA DIGITAL EN EL PROCESO PENAL DE CÓRDOBA

Tesis presentada por: **Esp. Mateo Pecchioni**

Directora de Tesis: **Dra. María Alejandra Sticca**

Tutor: **Esp. Franco Pilnik**

Maestría en Derecho Procesal

UESIGLO21 Córdoba 2024

AGRADECIMIENTOS

• Expreso mi sincero agradecimiento a la Dra. María Alejandra Sticca, mi directora de tesis, quien, desde mis días como estudiante universitario, me brindó la oportunidad de ser pasante en el C.I.J.S. (Centro de Investigaciones Jurídicas y Sociales). Ahora y en esta nueva etapa, con generosidad y dedicación, aceptó la responsabilidad de guiar mi tesis, brindándome orientación con su característica calidez humana.

• Reconozco con gratitud a mi tutor, Esp. Franco Pilnik, cuya profunda erudición me ha motivado a continuar explorando el campo de la cibercriminalidad, sus respuestas a mis interrogantes y su generosa orientación han sido invaluables.

• Quiero expresar mi agradecimiento a la Universidad Siglo 21 por proporcionarme el espacio necesario para mi desarrollo y formación profesional, su respaldo ha sido fundamental en esta etapa de crecimiento académico.

INDICE

CAPÍTULO SEGUNDO

MARCO LEGISLATIVO DE LA ESTAFA INFORMATICA Y LA PRUEBA DIGITAL

CAPÍTULO TERCERO

MARCO JURISPRUDENCIAL DE LA ESTAFA INFORMÁTICA Y LA PRUEBA DIGITAL

CAPITULO QUINTO

ACTORES DEL PROCESO

Resumen

Esta tesis se enfoca en el análisis exhaustivo de la prueba digital en el ámbito de los delitos de estafa informática dentro de la provincia de Córdoba. En cuanto al período temporal durante el cual se realizó la investigación, el mismo abarca un año calendario. Como parte del objeto de estudio se incorporaron datos previos o históricos comprendidos entre enero del año 2019 hasta diciembre del año 2023. Ante la notable proliferación de actividades delictivas en entornos digitales, se propone una investigación profunda sobre la valoración y utilización de la evidencia digital en el contexto del proceso penal Cordobés. La intersección entre la prueba digital y el fraude informático es explorada minuciosamente, considerando las condiciones necesarias para su admisión y ponderación en el escenario jurídico. Además, se aborda con meticulosidad el rol y las responsabilidades atribuidas a las unidades judiciales y entidades especializadas en el tratamiento de la prueba digital en casos de estafa informática. El presente trabajo académico se sumerge en la comprensión de la naturaleza y características inherentes a la prueba digital, y cómo estas interactúan con los requerimientos de la esfera penal. Un enfoque cualitativo se adopta para captar las voces y perspectivas de múltiples actores involucrados, igualmente, se lleva a cabo un minucioso análisis documental, que abarca desde informes y estudios previos hasta jurisprudencia y documentos legales que rigen la materia en la provincia de Córdoba.

Abstract

This thesis is centered on a comprehensive analysis of digital evidence within the domain of computer fraud offenses in the province of Córdoba. Regarding the study period, a research framework covering a calendar year has been defined, specifically from January 2022 to December 2023. In light of the significant rise in criminal activities within digital environments, this research proposes an in-depth investigation into the assessment and utilization of digital evidence within the context of the criminal process in Córdoba. The intricate intersection between digital evidence and computer fraud is meticulously examined, taking into account the necessary conditions for its admission and consideration within the legal framework, furthermore, the roles and responsibilities assigned to Judicial Units and specialized entities involved in the handling of digital evidence in cases of computer fraud are scrupulously addressed. This academic work delves into understanding the inherent nature and characteristics of digital evidence and how they interact with the requisites of the penal sphere. A qualitative approach is embraced to capture the perspectives and insights of various stakeholders, additionally, a meticulous documentary analysis is conducted, encompassing everything from previous reports and studies to legal precedents and legislative documents that govern the subject matter in the province of Córdoba.

ABREVIATURAS

ART: Artículo.

BPC: Banco de la Provincia de Córdoba.

CEPAL: Comisión Económica para América Latina y el Caribe.

CEDH: Convenio Europeo de Derechos Humanos.

CN: Constitución Nacional Argentino.

CP: Código Penal Argentino.

CPP: Código Procesal Penal.

CSC: Convenio sobre ciberdelincuencia.

DNS: Domain Name System (sistema de nombres de dominio).

ENISA: European Union Agency for Network and Information Security (Agencia Europea para la Red y la Seguridad de la Información).

Europol: Oficina Europea de Policía.

FTP: File Transfer Protocol (protocolo de transferencia de archivos).

HTTP: Hyper Text Transfer Protocol.

ICJ: Instituto de Cibercrimen de Córdoba.

IFE: Ingreso Familiar de Emergencia.

INDEC: Instituto Nacional de Estadística y Censos.

Interpol: Organización Internacional de Policía Criminal.

INC: Inciso.

IP: Internet Protocol.

ISP: Internet Service Provider (Proveedor de Servicios de Internet).

ITC: Instituto Tecnológico de Córdoba.

LAN: Local Area Network (Red de Área Local).

LO: Ley Orgánica.

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal.

LOPJ: Ley Orgánica del Poder Judicial.

MAC: Media Access Control (Control de Acceso de Medios).

MPF: Ministerio Público Fiscal.

NCP: Network Control Protocol (Protocolo de Control de Red).

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

NSF: National Science Foundation (Fundación Nacional para la Ciencia).

NSFNET: National Science Foundation Network (Red de la Fundación Nacional para la Ciencia).

OEDE: Orden Europea de Detención y Entrega.

OEI: Orden Europea de Investigación en Materia Penal.

ONL: Organización de las Naciones Unidas.

OEA: Organización de los Estados Americanos.

TAD: Trámites a Distancia.

TCP/: Transmisión Control Protocol

TIC: Tecnologías de la Información y la Comunicación.

TSJ: Tribunal Superior de Justicia.

UCI: Unidad de Cibercrimen de la Policía de Córdoba.

UCIJ: Unidad de Cibercrimen e Investigaciones Judiciales de Córdoba.

UFECI: Unidad Fiscal Especializada en Ciberdelincuencia.

VPN: Virtual Private Network (Red Privada Virtual).

I**ntroducción**

En el presente trabajo de investigación se aborda de manera detallada la relevancia de la prueba digital en el delito de estafa informática, en el contexto de los delitos cometidos en entornos digitales en la provincia de Córdoba.

El presente trabajo final es continuación del estudio realizado junto al fiscal de instrucción en Cibercrimen Franco Pilnik, director de la tesis titulada "Delitos Cometidos en Entornos Digitales: La estafa informática criterios generales y su relación con otras figuras delictivas" y publicado en la biblioteca virtual de la Academia de Derecho de la Universidad Católica de Córdoba (UCC), como trabajo final de la especialidad en derecho judicial y de la judicatura.

El trabajo elaborado junto al fiscal Franco Pilnik sirve como punto de partida para continuar investigando el fenómeno de la estafa informática y su crecimiento exponencial durante el aislamiento social y preventivo generado por la pandemia de COVID-19, abarcando como objeto de estudio los periodos comprendidos entre el año 2020 hasta el año 2022.

La continuidad de dicha investigación no solo nos permite profundizar en la comprensión de la dinámica delictiva en entornos digitales, sino también contribuir al fortalecimiento de las herramientas y estrategias necesarias para abordar eficazmente estos casos en el ámbito judicial.

Además, en esta tesis final, se dedicará especial atención a la problemática procesal relacionada a la incorporación de la prueba obtenida en el marco de ciberdelitos, especialmente en casos de estafa informática.

En la actualidad, el crecimiento exponencial de las tecnologías de la información y la comunicación ha dado lugar a incontables modalidades de estafas informáticas, lo que ha generado la necesidad de un análisis detallado sobre el tratamiento de la prueba digital en este tipo de delitos.

"La proliferación de este tipo de actividades delictivas en entornos digitales ha planteado un desafío crítico para los sistemas de justicia penal, que se enfrentan a la tarea de comprender y gestionar la prueba digital en este contexto" (Creswell, J. W. 2013).

La presente investigación se enmarca dentro del paradigma dogmático y adopta un enfoque cualitativo, considerándose de naturaleza exploratoria. Este enfoque se considera apropiado debido a la necesidad de comprender la realidad social del cibercrimen desde la perspectiva de los participantes. Explorar sus experiencias, significados y percepciones, y captar la complejidad del fenómeno estudiado, igualmente el enfoque cualitativo permitirá obtener una visión holística y detallada del cibercrimen, considerando sus dimensiones sociales, psicológicas y tecnológicas.

Desde una perspectiva favorable, es innegable que la prueba digital se ha convertido en un pilar esencial en la investigación y persecución de la estafa informática, así como lo plantea Rodríguez, G. (2002); "En el contexto de delitos cibernéticos, la prueba digital no solo es una herramienta útil, sino que a menudo es la única fuente confiable de evidencia".

"Los rastros digitales, registros electrónicos y comunicaciones en línea ofrecen un panorama completo de la actividad delictiva en el ciberespacio, en este sentido, la prueba digital es fundamental para establecer la culpabilidad de los perpetradores y garantizar una justicia efectiva" (Rodríguez, G., 2002).

No obstante, en el desarrollo del presente, se han enfrentado posiciones en contrario, existen aquellos que sostienen que el valor de la prueba digital es igual al de cualquier otro medio probatorio en el proceso penal. Autores como Rodríguez, C (2018) argumenta que no se debe otorgarse un estatus especial a la evidencia digital y que todas las pruebas, ya sean testimoniales, documentales o digitales, deben evaluarse bajo los mismos estándares, según esta perspectiva, no se

justifica una atención excesiva a la preservación y admisibilidad de la prueba digital en detrimento de otros medios de prueba[1].

La tesis en cuestión posee un valor intrínseco al explorar con profundidad cómo se valora la prueba digital en el procedimiento procesal penal de la provincia de Córdoba. En particular en el contexto de los delitos de estafa informática, siguiendo la perspectiva de destacados expertos en el campo legal, como Martínez R. (2019), se plantea una pregunta central que se torna fundamental en este estudio: ¿Cómo se incorpora la evidencia digital en el procedimiento procesal penal frente al delito de estafa informática?.

En este sentido, se formula la hipótesis de trabajo y se argumenta a favor de que una adecuada incorporación de la prueba digital en los casos de estafa informática en la provincia de Córdoba. No solo fortalecerá significativamente el sistema de justicia penal, sino que también aumentará sustancialmente la probabilidad de obtener sentencias condenatorias en este tipo de delitos.

Este razonamiento se sustenta en la premisa de que la correcta gestión y presentación de la evidencia digital, en estricta conformidad con los estándares y protocolos apropiados, desempeñará un papel crucial en la preservación de su integridad y veracidad.

Para lograr estos objetivos, esta investigación se estructura en diferentes capítulos, el primero establece el contexto histórico y geográfico de la investigación, delineando los límites espaciales y temporales, definiendo la temática de estudio. Además, se adentra en las nociones teóricas de prueba digital y de la estafa cometida en entornos digitales.

[1] Para profundizar en relación a esta posición en contrario y obtener una perspectiva más detallada sobre el valor de la prueba digital en el proceso penal, se recomienda consultar el trabajo de Rodríguez, C (2018) *pp. 45-62.*

El capítulo segundo se enfoca en el contexto internacional y comparativo, analizando la legislación y los convenios relevantes en materia de cibercrimen y prueba digital, para luego desarrollar el marco legislativo nacional y provincial, evaluando cómo se aborda la estafa informática y la prueba digital en el sistema legal de Córdoba.

Por su parte a lo largo del capítulo tercero se explora el marco jurisprudencial relacionado con la admisión e incorporación de la prueba digital en el proceso penal, tanto a nivel nacional como provincial.

El capítulo cuarto se explora la admisión e incorporación de la prueba digital en el proceso penal. Por último, el capítulo quinto presenta los sujetos y órganos del proceso, sus respectivas funciones y responsabilidades.

Finalmente, y a modo de cierre se presentan en el capítulo de la conclusión, las propuestas resultantes de la investigación, recomendaciones y en anexo una guía práctica novedosa.

CAPÍTULO PRIMERO
DESCRIPCIÓN DEL CONTEXTO HISTÓRICO

1.Introducción

El capítulo primero de esta investigación tiene como objetivo fundamental establecer un sólido contexto histórico y teórico que enmarque de manera precisa el estudio sobre la recepción de la prueba digital en el procedimiento procesal penal de la provincia de Córdoba frente al delito de estafa informática.

En este sentido, se enfocará en varios aspectos cruciales que sientan las bases para el análisis en profundidad que se llevará a cabo en los capítulos posteriores, uno de los objetivos específicos que se cumplirán en este capítulo es la delimitación rigurosa del contexto espacial y temporal de esta investigación, lo que implica definir a la capital de la provincia de Córdoba, Argentina, como el ámbito geográfico de enfoque de investigación.

La organización de este capítulo ha sido cuidadosamente planificada para abordar de manera coherente y secuencial una serie de aspectos claves, con una contextualización que abarca la descripción del contexto histórico y geográfico de la provincia de Córdoba. Luego, se llevará a cabo un análisis exhaustivo de las bases teóricas relacionadas con la prueba digital, seguido por una exploración de los distintos tipos de estafas informáticas. A continuación, se abordará la importancia de la introducción de la prueba digital en el proceso penal, se realizarán precisiones terminológicas esenciales y, finalmente, se procederá con la exploración detallada de los principales registros electrónicos pertinentes en este contexto.

Esta estructura permite un enfoque claro y sistemático en la construcción de los fundamentos necesarios para comprender a fondo la

recepción de la prueba digital en los casos de estafa informática en la provincia de Córdoba, Argentina, durante el período especificado.

La importancia trascendental de este capítulo radica en su capacidad para sentar cimientos sólidos y proporcionar una comprensión profunda de los antecedentes y conceptos clave necesarios para llevar a cabo un análisis riguroso de la incorporación de la prueba digital en los casos de estafa informática en la provincia de Córdoba, Argentina, durante el período mencionado.

Estos elementos son esenciales para contextualizar adecuadamente los desafíos y las oportunidades que enfrenta el sistema de justicia penal Cordobés en esta área en constante evolución, y, en última instancia, contribuir a un estudio comprehensivo y esclarecedor sobre esta temática.

Para alcanzar los estos objetivos, se emprenderá una exploración exhaustiva de las diversas modalidades de estafas informáticas que prevalecen en la provincia de Córdoba. Este análisis permitirá comprender la naturaleza de los delitos cibernéticos y su correlación con la evidencia digital, estableciendo así un fundamento sólido para la posterior evaluación de la valoración de la prueba en este contexto. Además, se analizará cómo la prueba digital se convierte en un elemento crucial en la investigación y persecución de estos delitos.

El cumplimiento de estos objetivos específicos constituye un paso esencial en la consecución del objetivo general de esta investigación: analizar y evaluar la recepción de la prueba digital en el procedimiento procesal penal de la provincia de Córdoba frente al delito de estafa informática.

Este capítulo proporcionará los cimientos necesarios para un análisis profundo y fundamentado en los capítulos subsiguientes.

1.1Delimitación espacial

El presente trabajo de investigación se lleva a cabo desde una perspectiva que permite estudiar la prueba digital en los delitos cometidos en entornos digitales. Con un enfoque especial en la estafa informática, esta perspectiva nos conduce a delimitar el ámbito geográfico de estudio al territorio bajo la jurisdicción del ministerio público fiscal de la provincia de Córdoba, Argentina (MPF).

En el universo de delitos cometidos en entornos digitales, donde la tecnología desempeña un papel central, es esencial concentrar nuestra atención en un contexto específico, por lo tanto, y a modo de punto de partida, la delimitación espacial se circunscribe a la provincia de Córdoba y, más concretamente, a su capital, la ciudad de Córdoba.

Esta elección geográfica no resulta aleatoria y se justifica por la relevancia que tiene en materia procesal penal, la incorporación de la prueba digital en el procedimiento, especialmente en los casos de estafa informática. El MPF de la provincia de Córdoba se encarga de investigar y perseguir los delitos en esta jurisdicción, lo que hace que esta área geográfica sea particularmente significativa para nuestro estudio. Además, esta delimitación nos permitirá considerar las dinámicas legales, judiciales y tecnológicas específicas que se manifiestan en Argentina.

La elección geográfica también trae aparejadas implicaciones prácticas, ya que nos facilitará la obtención de datos, la realización de entrevistas y el acceso a recursos y expertos locales relevantes para la presente investigación. Así, garantizamos que los resultados y las conclusiones que obtengamos estén directamente relacionados con el contexto legal y tecnológico de la provincia de Córdoba, lo que aumentará la aplicabilidad y la pertinencia de nuestro estudio en este ámbito geográfico específico

Finalmente, es importante destacar que esta investigación también considera la dimensión internacional de los delitos cometidos en entornos digitales, planteado por muchos autores como los desafíos adicionales en la investigación y persecución de estos delitos. (Pilnik, 2017)

Si bien el enfoque principal se encuentra en el ámbito geográfico de la provincia de Córdoba, Argentina, se hará mención y se tendrá en cuenta la naturaleza transnacional de estos delitos, reconociendo que las implicaciones y los aspectos internacionales también son parte integral de nuestro estudio.

1.2 Delimitación temporal

Respecto al período temporal durante el cual se realizó la investigación, como ya se ha mencionado anteriormente, el mismo abarca un año calendario. Como objeto de estudio se incorporaron datos históricos, del primer trimestre del año 2019 al último trimestre del 2020, obtenidos en la investigación llevada a cabo junto al fiscal de ciberdelitos de la provincia de Córdoba.

Esta elección temporal se ha realizado con el propósito de examinar minuciosamente los eventos y acontecimientos relacionados con la incorporación al proceso, de la prueba digital en casos de estafa informática, dentro del ámbito jurisdiccional de la provincia de Córdoba, Argentina.

Este período de investigación coincide con lo que se ha denominado el período pos pandémico, contexto ubicado temporalmente entre los años 2020 y 2022 y caracterizado por un marcado incremento en la incidencia de los delitos informáticos. Siendo de gran relevancia, el aislamiento social preventivo y obligatorio para evitar la circulación y el contagio del virus COVID-19, el cual desencadeno un aumento sustancial en la dependencia de la tecnología y la conectividad por parte de toda la

sociedad, dando lugar a la proliferación de actos delictivos en el ámbito digital. El propósito fundamental de este estudio radica en explorar y comprender el impacto de la pandemia en la dinámica de los delitos informáticos en la región de Córdoba.

La elección específica de este marco temporal, no resulta aleatoria, por el contrario, nos permitirá realizar un análisis exhaustivo de posibles modificaciones en la legislación, avances tecnológicos y tendencias en la comisión de delitos informáticos. Esto contribuirá a obtener una comprensión actualizada y contextualizada de la temática en el área geográfica definida, aspecto fundamental para abordar de manera efectiva los desafíos y oportunidades que plantea la incorporación de la evidencia digital en casos de estafa informática en el entorno socio-tecnológico contemporáneo.

1.2.1-El período Pos pandémico

Un dato revelador sobre la situación de los ciberataques en América Latina emerge a partir de la herramienta interactiva denominada Threat Intelligence Insider Latin América (TIILA)[2], desarrollada por Fortinet[3] en su primera edición en 2020, el que da cuenta que, entre abril y septiembre del mismo año, la región experimentó más de 100 billones de intentos de ciberataque.

2 T.I.I.L.A; publicación especializada en seguridad cibernética y análisis de amenazas en América Latina. Esta revista ofrece análisis exhaustivos, informes y noticias sobre las últimas tendencias, técnicas y herramientas relacionadas con la seguridad informática en la región.

3 Fortinet;empresa líder en ciberseguridad que ofrece soluciones integrales de seguridad de redes, incluyendo firewalls, sistemas de detección y prevención de intrusiones, seguridad de acceso remoto, entre otros productos y servicios relacionados con la protección de redes y datos.

Además de lo anterior y de acuerdo con el Istituto Analisi Relazioni Internazionali (IARI)[4] y el reporte[5]; Cyber crime in Latin América - Statistics & Facts de septiembre del 2022 realizado por Tiago Bianchi[6], el costo global del cibercrimen en todo el mundo se elevó a US$ 113 mil millones de dólares, con un estimado de 378 millones de víctimas anuales, lo cual equivale a la población total de América del Sur, esto se traduce en un promedio de 12 víctimas de ciberdelitos por segundo.

7

Por otro lado, el Observatorio de Delitos Informáticos de Latinoamérica (ODILA)[8] ha proporcionado datos reveladores; en

4 IARI; Instituto de análisis y estudio de relaciones internacionales con sede en Italia, lleva a cabo investigaciones relacionados con las relaciones internacionales, diplomacia, cooperación internacional, seguridad global y política exterior de los países.

5 Realizado por Tiago Bianchi durante la pandemia y publicado en mayo del 2023.

6Tiago Bianchi; investigador Brasileño de Statista, especializado en internet, con enfoque en América Latina y España, investigador del acceso, tráfico, redes sociales, empresas y los motores de búsqueda.

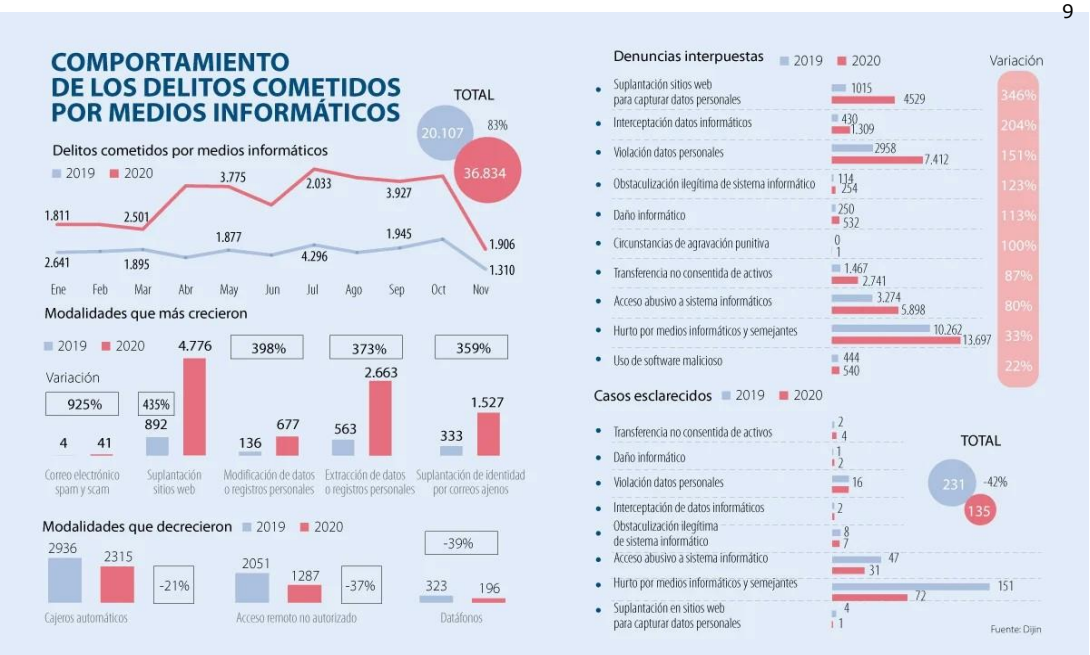
7 Gráfico extraído de https://www.asuntoslegales.com

8 ODILA: Iniciativa dedicada a monitorear, analizar y difundir información sobre los delitos informáticos en latinoamericana.

diecisiete países de la región, el ochenta y tres coma seis por ciento (83.6%) de los encuestados afirmaron no haber denunciado nunca haber sido víctimas de estafas informáticas, a pesar de haber experimentado tales incidentes. Sin embargo, lo que resulta aún más sorprendente es que, de cada cien delitos informáticos cometidos en América Latina, solo uno conduce a una sanción efectiva.

Esta brecha en la denuncia se atribuye en gran medida a la ausencia de estadísticas oficiales en esta materia, lo que representa un desafío sustancial para la formulación de estrategias de combate al cibercrimen a largo plazo. Entre los motivos que disuaden de la denuncia se encuentran la desconfianza en la capacidad del sistema penal para abordar estos delitos y el temor a la pérdida de confidencialidad al hacer públicos estos incidentes. En línea con las conclusiones de la herramienta T.I.I.L.A de Fortinet, el ODILA señala que el tipo de delito más reportado es el phishing y con las diversas variantes de estafa informática.

9



9 Gráfico extraído de https://www.asuntoslegales.com

Por último, se dispone de datos recopilados por Google y analizados por Atlas VPN[10], los cuales arrojan luz sobre la magnitud de este fenómeno. En enero del 2020, Google registró ciento cuarenta y nueve mil ciento noventa y cinco (149195) sitios web activos de phishing, este número se aproximadamente se duplicó en febrero del mismo año, llegando a doscientos noventa y tres mil, doscientos treinta y cinco (293235) sitios activos. En marzo del mismo año, el número de estafas crecieron aún más, alcanzando los quinientos veintidós mil cuatrocientos noventa y cinco (522495) sitios web activos de phishing, lo que supone un aumento del trescientos cincuenta por ciento (350%) desde enero del 2020.

11

10 Proveedor de servicios VPN (Red Privada Virtual) que ofrece una variedad de funciones de seguridad y privacidad en línea.

11 Gráfico extraído de https://transparencyreport.google.com/safe-browsing/search

De acuerdo con la unidad fiscal especializada en ciberdelincuencia (UFECI)[12], uno de los cambios más notables que la pandemia desencadenó fue el aumento significativo en el número de usuarios bancarizados. Durante el período de aislamiento social, preventivo y obligatorio, se crearon millones de nuevas cuentas bancarias, también llamadas billeteras virtuales, telefónicas o digitales, muchas veces para acceder a programas gubernamentales como el Ingreso Familiar de Emergencia (IFE)[13].

Esta expansión en la bancarización también trajo consigo un incremento en los casos de robo de claves de acceso a servicios de banca en línea y datos de tarjetas de crédito, delitos que experimentaron un aumento exponencial durante el año 2020.

Durante este período, se produjeron millones de ciberataques en Argentina, lo que sugiere que las estafas virtuales se multiplicaron como un virus. Entre las víctimas más afectadas se encuentran los nuevos usuarios de servicios de home-banking[14], y las modalidades más comunes de estafa informática son el phishing[15] y el malware[16].

Un factor que contribuye significativamente a esta tendencia es el continuo desarrollo de las tecnologías de la información y la

12 División del ministerio público fiscal dedicada a investigar y perseguir los delitos informáticos y cibernéticos en el país, creada en 2017 como respuesta a la creciente incidencia de delitos en el ámbito digital.

13 Seguro social de Argentina que se entregó a trabajadores informales y monotributistas de las primeras categorías durante la emergencia debido a la pandemia de enfermedad por coronavirus

14 Uso de servicios bancarios a través de internet desde la comodidad del hogar o cualquier otro lugar con acceso a la red. También conocido como "banca en línea" o "banca por Internet"

15 Técnica de ingeniería social utilizada por ciberdelincuentes para obtener información confidencial o comprometer sistemas informáticos.

16 Malware, abreviatura de "software malicioso", se refiere a cualquier programa diseñado para causar daño a una computadora, servidor, cliente o red informática.

Comunicación (TIC)[17] y su creciente adopción por parte de la sociedad, las TIC se han integrado cada vez más en la vida cotidiana de una gran parte de la población, según los datos[18] del Instituto Nacional de Estadística y Censos (INDEC)[19], para el último trimestre del 2020, el ochenta y seis por ciento (86%) de la población en Argentina utilizaba una conexión internet, este aumento del cinco coma seis por ciento (5.6%) en comparación con el año anterior refleja una tendencia al alza en el acceso a Internet y, por ende, a los servicios proporcionados en línea.

Sin embargo, el impacto de la pandemia en el uso de las TIC fue aún más pronunciado a partir de marzo del 2020, cuando las medidas de prevención impulsaron una mayor adopción de la tecnología por parte de la población. Empresas como Mercado Libre[20] informaron a través de portal Statista GmbH[21] el aumento del cuarenta por ciento (40%) en la cantidad de usuarios nuevos registrados en su plataforma de comercio electrónico y un crecimiento del setenta y uno por ciento (71%) en los pagos de servicios a través de Mercado Pago[22].

17 (TIC) conjunto de herramientas, recursos y sistemas que facilitan la adquisición, almacenamiento, procesamiento, transmisión y presentación de información a través de dispositivos electrónicos y redes de comunicación.

18 Publicados en la página oficial - https://www.indec.gob.ar/indec/web/Institucional-Indec-NoticiasCovid-4.

19 Organismo encargado de producir y difundir estadísticas oficiales en Argentina, Creado en 1968 y dependiente del Ministerio de Economía y Finanzas Públicas.

20 Empresa multinacional Argentina dedicada al comercio electrónico en Latinoamérica.

21 Portal de estadística en línea alemán que pone al alcance de los usuarios datos relevantes que proceden de estudios de mercado y de opinión, así como indicadores económicos y estadísticas oficiales en alemán, inglés, español y francés.

22 Plataforma de cobros online de Argentina, la herramienta permite cobrar por Internet a través de diferentes opciones y modos.

Estudios realizados por Google[23] durante la pandemia también señalaron que casi un tercio de los argentinos que compraron en línea durante ese período lo hicieron por primera vez, y que la mitad de los compradores optaron por las compras en línea para minimizar la exposición en entornos físicos.

Por su parte, el Banco Central de la República Argentina (BCRA) informó a través de su portal web[24], que las operaciones electrónicas aumentaron un diecinueve por ciento (19%) en 2020 en comparación con el año anterior, con un aumento significativo en las operaciones de homebanking ochenta y seis por ciento (86%), mobilebanking ciento sesenta y siete por ciento (167%) y los pagos remotos con tarjeta de débito doscientos veintisiete por ciento (227%). Estos datos también se reflejaron en el estudio anual del año 2020 de la cámara Argentina de comercio electrónico, que informó un aumento interanual del ciento veinticuatro por ciento (124%) en la facturación y del ochenta y cuatro por ciento (84%) en la cantidad de órdenes de compra en línea.

Igualmente, de los aspectos comerciales y financieros, numerosos organismos y empresas facilitaron la realización de trámites y operaciones en línea durante los períodos de aislamiento y distanciamiento social.

Las nuevas tecnologías han revolucionado la forma en que llevamos a cabo una amplia gama de actividades cotidianas, permitiendo su realización desde la comodidad del hogar, este fenómeno ha cobrado una relevancia especial en el contexto de la pandemia, donde las medidas de confinamiento y distanciamiento social han llevado a un aumento significativo en la adopción y el uso de estas tecnologías. Cobra

---

23 Empresa tecnológica multinacional conocida principalmente por su motor de búsqueda en línea

24 Información y medidas adoptadas por el BCRA - https://www.bcra.gob.ar/noticias/coronavirus-BCRA.asp

sentido que el empleo creciente de las tecnologías de la información y la comunicación (TIC) haya dado lugar a un incremento considerable en la cantidad de interacciones y transacciones que pueden ser objeto de maniobras delictivas en línea.

En el marco de la pandemia, organismos internacionales con competencia en la materia, como la Organización Internacional de Policía Criminal (Interpol)[25], la Oficina Europea de Policía (Europol)[26], la Organización de los Estados Americanos (OEA)[27] y la Comisión Económica para América Latina y el Caribe (CEPAL)[28] de la Organización de las Naciones Unidas (ONU)[29], entre otros, han observado una correlación entre los nuevos patrones de comportamiento generados por la crisis sanitaria y el aumento de actividades delictivas en el ciberespacio a nivel global, estas instituciones han identificado una relación directa entre la adopción masiva de tecnologías digitales debido al distanciamiento social y el incremento de casos de delitos informáticos.

Para analizar en detalle esta tendencia, tomamos las estadísticas aportadas por Statista GmbH y publicada en su portal de Statista Research Department[30], en relación con el primer trimestre de pandemia de los años 2019, 2020 y 2021.

En el primer trimestre de 2019, se registraron un total de quinientos ochenta y uno (581), reportes relacionados con delitos informáticos, este

25 Organización Internacional de Policía Criminal, entidad que facilita la cooperación policial internacional, fundada en 1923.

26 Oficina Europea de Policía, agencia de la Unión Europea (UE) -fue fundada en 1998.

27 Organización de los Estados Americanos (OEA) organismo internacional, fundado el 30 de abril de 1948.

28 Organismo regional de las Naciones Unidas, establecida en 1948.

29 Organización de las Naciones Unidas (ONU), fundada el 24 de octubre de 1945

30https://es.statista.com/estadisticas/1105121/numero-casos-covid-19-america-latina-caribe-pais/

aumento, que representó aproximadamente un treinta y seis por ciento (36%) de incremento, ocurrió en los dos trimestres anteriores a la implementación de medidas relacionadas con la pandemia de COVID-19 en Argentina. Esta variación podría explicarse por diversos factores, se encuentra en línea con la tendencia previa de un aumento sostenido en los casos de cibercriminalidad.

Sin embargo, el primer trimestre del 2021, ya afectado por la pandemia y las medidas de prevención correspondientes, experimentó un aumento aún más pronunciado en la cantidad de reportes. En este período, se reportaron un total de tres mil novecientos setenta y seis (3976) casos, lo que representa un aumento del Cuatrocientos tres por ciento (403%), en comparación con el mismo período del año 2020, esta discrepancia significativa subraya la influencia directa de la pandemia y sus consecuencias en el aumento de la delincuencia informática.

Es importante destacar que el número de reportes[31] de delitos informáticos parece estar directamente relacionado con el aumento de la actividad delictiva en línea, que, a su vez, se correlaciona con el crecimiento y la adopción de las tecnologías de la información y la comunicación. En este sentido, el incremento en la cantidad de reportes está vinculado a un factor concomitante, con un potencial disruptivo significativo: las medidas de aislamiento social y los nuevos hábitos sociales que surgieron como resultado de la pandemia.

La crisis sanitaria del periodo pandémico, no sólo impulsó el uso masivo de las TIC en la sociedad, sino que también aceleró la adaptación de diversas actividades a entornos digitales. Esto se vio reflejado en el hecho de que un gran número de organismos gubernamentales y empresas han promovido la realización de trámites y operaciones en línea durante los períodos de aislamiento y distanciamiento social, la

31 Statista Research Department - https://es.statista.com/temas/6298/el-nuevo-coronavirus-covid-19-en-america-latina/#topicOverview

plataforma Trámites a Distancia (TAD)[32] experimentó un incremento del ciento treinta por ciento (130%) en la cantidad de usuarios registrados durante la pandemia, junto con aumentos significativos en la generación de trámites en línea y la producción de documentos digitales en la plataforma.

Además, el teletrabajo, originalmente vinculado a las TIC, se consolidó como una modalidad laboral en diversos sectores durante la pandemia, se estima que el número de personas empleadas que trabajaban desde sus hogares superó el millón trescientos sesenta y cuatro mil sesenta y seis (1,364,066) en el tercer trimestre del 2020, en comparación con las doscientos doce mil trescientos ochenta (212,380) estimadas para el primer trimestre del mismo año.

En síntesis, el aumento en los reportes de delitos informáticos en el contexto de la pandemia refleja una relación intrínseca entre el uso intensivo de las tecnologías digitales, las medidas de aislamiento y distanciamiento social, y el incremento en actividades delictivas en línea, destaca este fenómeno y la correspondiente necesidad de abordar la ciberseguridad como un componente fundamental de la respuesta global ante los desafíos emergentes en el ámbito digital.

1.3 Temática y unidad de análisis

La temática central de esta investigación se sitúa en la confluencia de dos ámbitos cruciales en la esfera jurídica y tecnológica: la incorporación de la prueba digital y los delitos informáticos, con un enfoque específico en los casos de estafa informática en la provincia de Córdoba, Argentina.

32 Plataforma donde cualquier ciudadano puede realizar su trámite ante organismos públicos nacionales desde su casa, oficina y/o dispositivo móvil https://tramitesadistancia.gob.ar/#/inicio.

Asimismo, la unidad de análisis primordial de este estudio recae en la evaluación exhaustiva de los procedimientos y prácticas relacionados con la prueba digital en el contexto de los procesos penales vinculados a los delitos cibernéticos en nuestra jurisdicción. En este aspecto, se pretende desentrañar la complejidad de la recolección, preservación y presentación en juicio de la evidencia digital, así como su ponderación en la toma de decisiones judiciales en casos específicos de estafa informática.

La unidad de análisis se extiende a los actores clave involucrados en este proceso, incluyendo los fiscales, jueces, abogados, peritos forenses y expertos en tecnología de la información, sin embargo la presente investigación también se adentrará en la normativa legal y las tendencias jurisprudenciales relacionadas con la materia, así como en la interacción de factores tecnológicos y legales que convergen en la resolución de casos de estafa informática en el contexto mencionado, esta unidad de análisis rigurosa y multidimensional servirá como base para un análisis completo y contextualizado de la recepción de la prueba digital en el ámbito penal en constante evolución.

1.4 Antecedentes - Marco teórico

Para fundamentar el presente trabajo de investigación, se presentarán los antecedentes y el marco teórico, esto incluirá una exploración de las bases teóricas relacionadas con la prueba judicial digital, las nociones teóricas que sustentan la comprensión de la estafa informática y sus distintos tipos y subtipos. Así también, como las precisiones terminológicas sobre las pretensiones que involucran prueba electrónica, estos fundamentos teóricos servirán como cimientos sólidos para el análisis y la interpretación de los hallazgos de la investigación.

Previo ingresar en el análisis de la prueba digital en el delito de estafa informática, será fundamental repasar los antecedentes

legislativos internacionales, nacionales y locales, en materia de delitos cometidos en entornos digitales y el abordaje de la prueba digital.

El punto de partida será la *Convención de Budapest sobre Cibercrimen*[33] la cual proporciona directrices para la investigación y el enjuiciamiento de delitos informáticos (Consejo de Europa, 2001), a nivel nacional, la Ley N° 26.388 será el objeto de estudio, la cual estableció disposiciones sobre delitos informáticos, incluyendo la obtención y valoración de la prueba digital en casos de estafa informática (Ditton, J., & Short, E. 2019). Es importante señalar en el caso del presente trabajo final se estudiará la normativa de delito informáticos, dentro del territorio de la provincia de Córdoba.

En el caso de la provincia de Córdoba, va a ser primordial el estudio de la regulación, tratamiento, normativas y protocolos específicos para la recolección, preservación y presentación de la evidencia digital en el marco del proceso penal.

Asimismo, resulta crucial analizar lo desarrollado en correspondencia a la materia objeto de estudio, ya que diversos autores han abordado la temática de la prueba digital en el delito de estafa informática desde diferentes enfoques.

En su artículo Gómez A. (2018) explora los aspectos técnicos y jurídicos de la evidencia digital, analizando sus características, su valor probatorio y los desafíos que implica su tratamiento en el ámbito penal. Por su parte, López J. (2020), investiga la evolución normativa y jurisprudencial en cuanto a la prueba digital, analizando la forma en que los tribunales han abordado su admisibilidad y valoración en estos casos. Martínez (2020), hace lo propio y examina las políticas y programas implementados a nivel local y nacional para prevenir y combatir los delitos

[33] También conocida como el Convenio del Consejo de Europa sobre Cibercriminalidad - adoptada el 23 de noviembre de 2001 en Budapest, Hungría, y entró en vigor en el año 2004.

informáticos, y destaca la importancia de la prueba digital en este contexto.

En la misma línea, Rodríguez (2018) analiza el enfoque y las perspectivas relacionadas con el manejo de la prueba digital en el proceso penal, especialmente en los casos de estafa informática.

En este mismo sentido, consideramos esencial el análisis de los trabajos doctrinarios que se utilizarán como norte del presente; siendo relevante lo que plantea García Ávila (2019), quien desarrolla cómo la prueba electrónica ha surgido como un elemento crucial en la administración de justicia en la era digital, particularmente en el contexto del proceso penal español.

García Ávila (2019) explica que:

> La prueba electrónica se refiere a cualquier tipo de evidencia digital que se utiliza para sustentar o refutar las acusaciones en un caso, esto incluye, entre otros, correos electrónicos, mensajes de texto, registros de llamadas, imágenes, videos, metadatos y datos extraídos de dispositivos electrónicos.
>
> La utilización de esta prueba electrónica ha planteado desafíos y oportunidades tanto para los tribunales como para las partes involucradas en el proceso penal. La introducción de la prueba electrónica en el proceso penal español implica considerar aspectos legales, técnicos y procedimentales. En el ámbito legal, se deben establecer las bases para la admisión y valoración de la prueba electrónica, garantizando su autenticidad, integridad y fiabilidad, y asegurando que se respeten los derechos fundamentales de las

partes, como el derecho a la defensa y la protección de la privacidad. (pp. 45-46)

Desde el punto de vista técnico, el trabajo de García Ávila desarrolla las capacidades y herramientas especializadas para la gestión, extracción, presentación y análisis de la prueba electrónica, lo cual implica la implementación de sistemas y software forenses, así como la formación de expertos en tecnología forense digital para garantizar la adecuada manipulación y preservación de la evidencia electrónica. En cuanto a los aspectos procedimentales, el autor explica cómo se deben establecer reglas y directrices claras sobre la presentación y utilización de la prueba electrónica en el proceso penal, lo cual incluye la adopción de procedimientos para la obtención legal de la evidencia digital, la cadena de custodia, la impugnación y la valoración de la prueba electrónica durante el juicio.

Finalmente, García Ávila concluye que:

> La introducción de la prueba electrónica en el proceso penal español ha llevado a una transformación en la forma en que se maneja la evidencia en los casos penales. Su incorporación ha requerido ajustes en los aspectos legales, técnicos y procedimentales para garantizar su recepción y apreciación adecuada. La gestión efectiva de la prueba electrónica en el proceso penal es fundamental para asegurar una justicia eficiente y equitativa en la era digital. (p. 67)

Por su parte, Chilcon (2019) desarrolla cómo el cibercrimen ha emergido como una amenaza significativa en todo el mundo, y el Perú no es una excepción. El autor explica que:

> El rápido avance de las tecnologías de la información y la comunicación ha llevado a un aumento en los delitos cibernéticos, que

van desde el robo de información personal y financiera hasta el ciberespionaje y los ataques cibernéticos a infraestructuras críticas. En el contexto de la seguridad nacional, el cibercrimen puede tener consecuencias graves y económicamente perjudiciales para todos los gobiernos. Los ataques cibernéticos dirigidos a instituciones gubernamentales, sistemas de defensa y servicios críticos pueden comprometer la soberanía del país, la estabilidad económica y la seguridad ciudadana. (p. 89)

Para abordar este problema, Chilcon sostiene que es crucial contar con políticas y estrategias de seguridad cibernética efectivas, lo cual implica el fortalecimiento de la legislación y las capacidades de aplicación de la ley, la promoción de la colaboración entre los sectores público y privado, y el desarrollo de capacidades técnicas y de concienciación en materia de ciberseguridad. Además, expone que:

Es importante fomentar la cooperación internacional en la lucha contra el cibercrimen, ya que muchas de estas actividades delictivas trascienden las fronteras nacionales. La participación en foros y acuerdos internacionales sobre ciberseguridad puede ayudar a fortalecer las capacidades y compartir información relevante para prevenir y combatir el cibercrimen de manera más efectiva. (p. 102)

Finalmente, y a modo de conclusión, Chilcon explica que:

El cibercrimen representa una amenaza significativa para la seguridad nacional en el Perú y en todo el mundo. La adopción de políticas y estrategias integrales de ciberseguridad, junto con la

cooperación internacional, son fundamentales para salvaguardar los intereses nacionales. (p. 110)

Por último, es relevante lo desarrollado por Cornavaca (2021), quien expone sobre la introducción de la prueba electrónica en el proceso civil. La autora explica que:

> En el contexto del proceso civil, la prueba electrónica se refiere a la evidencia que se presenta en formato digital, tal como correos electrónicos, documentos electrónicos, registros electrónicos, grabaciones de audio y video, entre otros. La incorporación de esta prueba electrónica plantea desafíos para todos los tribunales civiles y partes involucradas (empleados, magistrados, peritos, abogados particulares, damnificados, compañías aseguradoras, etc.). (p. 56)

Cornavaca (2021) se sumerge en la introducción de la prueba electrónica en las audiencias de Córdoba y todas sus implicancias legales, técnicas y procedimentales. La autora desarrolla las normas y regulaciones específicas que rigen el uso de la prueba electrónica en las audiencias civiles en la provincia de Córdoba capital. En términos técnicos, Cornavaca aborda cómo se deben establecer mecanismos y sistemas para la presentación y reproducción adecuada de la prueba electrónica durante las audiencias.

> Desde una perspectiva procedimental, la introducción de la prueba electrónica requiere ajustes en los procesos y prácticas existentes, lo cual puede incluir la adopción de nuevas reglas y procedimientos para la presentación, refutación y apreciación de la prueba electrónica, así como la protección de la confidencialidad y privacidad de la información contenida en dicha prueba. (p. 70)

Finalmente, el trabajo sobre la introducción de la prueba electrónica en el proceso civil por audiencias de Córdoba implica:

> La adaptación de los sistemas legales, técnicos y procedimentales para abordar el uso y recepción de la evidencia digital. Esto requiere una comprensión integral de los desafíos y encrucijadas asociados con la prueba electrónica, y el desarrollo de marcos normativos y prácticas adecuadas para garantizar el manejo adecuado en las audiencias civiles llevadas a cabo en la Docta. (p. 82)

Finalmente, y como consecuencia de los anteriores análisis, nos toca alcanzar el tema controversial del presente trabajo de investigación, esto es; la admisibilidad de la evidencia digital en materia especifica de la estafa informática.

Aquí radica nuestra mayor dificultad, ya que, dentro del ámbito de la prueba digital en materia penal, entre diversos autores existe una controversia en torno a la admisibilidad y el valor probatorio de la evidencia digital.

En el contexto de esta investigación, se presenta un debate de gran relevancia en torno a la admisibilidad de la evidencia digital en los casos de estafa informática. Esta discusión ha sido abordada por diversos autores, entre los que se destaca la postura de Rodríguez, C (2018) y Gómez L. (2017), quienes plantean argumentos que cuestionan la necesidad de otorgar un estatus especial a la evidencia digital en los procesos judiciales.

Según las perspectivas defendidas por los autores, se postula que:

> No se justifica la concesión de un estatus singular a la evidencia digital, abogando porque todas las pruebas presentadas ante un tribunal, independientemente de su naturaleza (ya sean

testimoniales, documentales o digitales), deben ser sometidas a una evaluación bajo los mismos estándares de admisibilidad y valor probatorio. Esta perspectiva sugiere que no es apropiado conferir una atención excesiva a la preservación y admisibilidad de la prueba digital en detrimento de otros medios de prueba, en parte debido a la inherente susceptibilidad de la evidencia digital a la manipulación y la falsificación. Por tanto, se argumenta que se debe abordar con precaución y rigor la evaluación del valor probatorio de la evidencia digital en los juicios, en vista de los desafíos técnicos y legales que pueden suscitarse y que plantean dudas sobre la autenticidad y la integridad de dicha evidencia. (p. 368)

Por otro lado, se encuentran autores, como Pérez A. (2022) y otros defensores del tratamiento especial de prueba digital, quien enfatiza en cuanto a la importancia de reconocer y valorar la relevancia de esta modalidad de prueba. Pérez A, argumenta que:

Es esencial adaptar el sistema judicial a los avances tecnológicos, subrayando la existencia de herramientas y técnicas forenses confiables que permiten una adecuada autenticación y preservación de la evidencia digital. Según esta perspectiva, el rechazo o la subestimación de la prueba digital podría limitar la capacidad de los tribunales para investigar y perseguir delitos informáticos, lo que podría generar impunidad y debilitar la efectividad de la justicia en el contexto digital. Este debate, por ende, plantea cuestiones fundamentales que abordan la intersección entre la tecnología y el derecho, y la necesidad de encontrar un equilibrio adecuado entre la

admisibilidad de la evidencia digital y la garantía de su autenticidad e integridad en el proceso penal. (pp. 240-259)

Otra arista del presente, sobre la cual se busca hacer especial foco, es la discrepancia que trae la ponderación de la privacidad y los derechos individuales en lo que respecta a la obtención y el uso de la prueba digital. Algunos escritores enfatizan la importancia de proteger la privacidad y los derechos de las personas en el contexto digital, argumentando que, la obtención y el análisis de la evidencia digital pueden implicar una intrusión desproporcionada en la esfera privada de los individuos (Rodríguez, 2018).

Sin embargo, existen otros académicos que consideran que, en casos de delitos informáticos, la obtención y el uso de la prueba digital son fundamentales para garantizar la persecución efectiva de los responsables y proteger a las víctimas, argumentando que, la importancia de combatir los delitos informáticos y salvaguardar la seguridad digital justifica en ciertas circunstancias la limitación de la privacidad y los derechos individuales (Torres, H. W. 2020).

Estas controversias y discrepancias en torno a la admisibilidad y la ponderación de la privacidad en la prueba digital en materia de estafa informática reflejan algunos de los grandes desafíos del presente trabajo de investigación.

1.5 Bases Teóricas

En el siguiente apartado, nos adentraremos en un análisis exhaustivo de los conceptos fundamentales relativos a la prueba judicial digital y a la estafa informática, paralelamente y a lo largo del capítulo segundo, examinaremos las disposiciones sustantivas que rigen el manejo legal de la evidencia electrónica en lo relativo a la este delito informático, abordando sus implicaciones en el ámbito del derecho procesal penal.

1.5.1 Nociones teóricas de prueba judicial digital

Como aspecto preliminar, resulta necesario establecer que, para los propósitos de la presente investigación, se considerarán intercambiables los siguientes términos: prueba judicial digital, prueba informática, y prueba electrónica, en estricta concordancia con el uso predominante atribuido a dichos términos por la mayoría de la doctrina jurídica nacional. (Aboso, G. E., & Zapata, M. F. 2006 y Palazzi, 2009; entre otros). No obstante, lo anterior, y a los fines del presente, se privilegia la utilización del término prueba judicial digital, dado que se estima que esta denominación refleja de manera integral la temática que se aborda en el presente trabajo de investigación.

Ahora bien, resulta imperativo abordar de manera primordial la construcción conceptual de la prueba judicial digital, ya que esta se erige como un pilar fundamental en el desarrollo del presente trabajo de investigación. En ese marco, resulta pertinente adentrarnos en la obra de grandes autores referentes en el ámbito de la prueba judicial, quienes han legado valiosas perspectivas que nos permitirán extraer y comprender a profundidad las facetas cruciales del concepto de prueba judicial digital, de esta forma podremos adquirir una comprensión más sólida y precisa de lo que implica la prueba judicial digital.

Así, Oneca, A. (2002), define a la prueba judicial como:

> Por prueba digital o electrónica cabe entender toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio, destacando los siguientes elementos; se refiere a cualquier clase de información, ha de ser producida, almacenada o transmitida por medios electrónicos, debe tener efectos para acreditar hechos en el proceso. (p. 70)

Pérez A. (2022) la define como:

> La prueba digital es la comprobación de las afirmaciones, el elemento indispensable de la demostración de la razón en el debate, medio de verificación de la verdad histórica de los hechos, de la verdad material de lo alegado por las partes. (p. 251)

Por su parte, M. Rivolta (2007) la define como: Se entiende por evidencia digital a los datos que constan en formato electrónico y que constituyen elementos de prueba, comprendiendo las etapas de extracción, procesamiento e interpretación.

A pesar de las notables diferencias apreciables en las definiciones esbozadas anteriormente, surge una característica esencial inherente a la institución probatoria: la búsqueda inquebrantable de la verdad, específicamente en correlación a los hechos que suscitan desacuerdos entre las partes, hechos que revisten una importancia determinante en lo que respecta a la vindicación de lo reclamado, este empeño por esclarecer la verdad se lleva a cabo, no obstante, dentro de los confines y restricciones que establece la legislación procesal penal.

Estas limitaciones legales no son meramente un mero trámite, sino que se encuentran intrínsecamente vinculadas a una plétora de propósitos igualmente sagrados y amparados por el derecho, entre ellos, se destaca la salvaguarda de derechos individuales de carácter fundamental, como el derecho a la intimidad, el respeto a la dignidad humana, el fiel cumplimiento del debido proceso legal y la aplicación inquebrantable del principio de igualdad ante la ley, entre otros.

Por ende, el cotejo entre la búsqueda de la verdad y el respeto a estos derechos constituye una delicada y compleja balanza que el sistema legal se esfuerza por mantener en equilibrio, para asegurar una justa y equitativa administración de la justicia en el ámbito del proceso penal.

1.5.2 Nociones teóricas de estafa informática

A los fines del presente trabajo, el punto de partida será lo dispuesto por el Código Penal de Argentina, el cual por Ley 26.388 introdujo, a través de su Artículo 9º, el inciso 16 del artículo 172, el cual define la estafa informática como: El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos.

Buompadre (2017) argumenta que esta nueva modalidad constituye una figura especializada en correspondencia con la estafa prevista en el artículo 172 del código penal, debido al medio empleado (un sistema informático).

Antes de esta nueva modalidad, se había contemplado la posibilidad de cometer fraude utilizando tarjetas de compra, débito o crédito sustraídas o extraviadas, incluso si se realizaban mediante operaciones automatizadas, según lo establecido en el artículo 173, inciso 15, incorporado por la Ley 25.390.

1.5.3 Tipos y subtipos de estafas informáticas

En el contexto de las estafas informáticas, es pertinente identificar varios tipos y subtipos de estos delitos cometidos en entornos digitales. A continuación, se explican algunos de los penalmente más relevantes:

Phishing: El phishing representa un conglomerado de estrategias diseñadas para engañar a individuos, suplantando identidades de confianza, como personas, empresas o servicios de prestigio, con el fin de persuadir a las víctimas para que ejecuten acciones perjudiciales. Estos ardides se valen de técnicas de ingeniería social y de la manipulación de las emociones humanas, con el potencial de dar lugar a la instalación de software malicioso, la alteración de sistemas o la sustracción fraudulenta de recursos financieros mediante engaños.

Email Phishing: En calidad de derivación del phishing, esta modalidad de estafa se traduce en el envío de correos electrónicos fraudulentos que aparentan provenir de fuentes legítimas, tales como entidades bancarias, comercios en línea u organismos gubernamentales. Estos mensajes suelen incorporar hipervínculos hacia sitios web fraudulentos que emulan la apariencia de las páginas auténticas, con el propósito de inducir a los destinatarios a revelar información personal o financiera. Asimismo, es factible que se adjunten archivos perniciosos con el fin de infectar dispositivos y posibilitar el acceso no autorizado a datos.

Spear Phishing: Constituye una variante refinada del phishing, caracterizada por la realización de una previa investigación sobre las víctimas, a menudo a través de plataformas de redes sociales, con miras a potenciar la credibilidad del atacante al dirigirse específicamente a individuos previamente identificados.

Whaling: Análogamente al phishing, pero focalizado en directivos y ejecutivos de alto rango en empresas. La escasa disposición de empresas y ejecutivos a denunciar estos casos suele obedecer al riesgo de desprestigio asociado.

Vishing: Fusión de las palabras "voice" (voz en inglés) y "phishing". En esta modalidad, los delincuentes realizan llamadas telefónicas para solicitar información personal, a menudo empleando grabaciones que simulan ser entidades financieras u oficinas gubernamentales. El propósito generalmente consiste en obtener contraseñas bancarias.

Typosquatting: Esta variante implica la creación de direcciones web que son similares a las legítimas, pero que contienen errores tipográficos sutiles que pueden pasar inadvertidos. Los ciberdelincuentes emplean esta táctica para redirigir a las víctimas hacia sitios web falsificados que emulan a los originales.

Resulta relevante subrayar que cada uno de los tipos y subtipos de estafas informáticas antes identificados presentan su propia

complejidad en lo que concierne a la obtención y el tratamiento de la evidencia digital conexa. La recolección de pruebas en el ámbito digital se erige como un desafío significativo, en vista de que los perpetradores de estas estafas a menudo operan en el anonimato y emplean técnicas de ocultación altamente sofisticadas, la autenticidad y la integridad de la evidencia, asimismo, pueden ser objeto de cuestionamientos, lo que impone la necesidad de un riguroso proceso de preservación y análisis forense digital, en estricta concordancia con los procedimientos y regulaciones vigentes en cualquier jurisdicción.

Adicionalmente, la incorporación y el uso efectivo de esta evidencia en un proceso judicial demandan un conocimiento especializado y la estricta observancia de los estándares legales propios de cada legislación. La lucha contra las estafas informáticas no solo exige salvaguardar contra estos delitos, sino también el desarrollo de capacidades sólidas en el ámbito de la ciberseguridad y la ciberforense para asegurar la eficacia de la justicia en el entorno digital, de acuerdo con las disposiciones de nuestro derecho procesal como continuaremos desarrollando.

1.6 Precisiones terminológicas de prueba electrónica.

En esta sección, es imperativo esclarecer y definir con rigurosidad los términos y conceptos fundamentales que gravitan en torno a las pretensiones legales que requieren la utilización de evidencia electrónica, estas precisiones terminológicas constituyen un pilar fundamental para asegurar una interpretación meticulosa y erudita de los casos de estafa informática, así como su adecuada gestión en el ámbito legal de la provincia de Córdoba.

A continuación, se presentan definiciones y aclaraciones terminológicas:

Evidencia electrónica: La evidencia electrónica, en el contexto jurídico, abarca un conjunto diverso de datos y registros digitales susceptibles de ser utilizados como pruebas en procesos legales, como apunta Charmaz, K. (2014). Esto puede englobar desde correos electrónicos, documentos electrónicos y sitios webs encriptados, hasta registros de transacciones financieras en línea y metadatos asociados a archivos digitales. La evidencia electrónica adquiere un papel central en el esclarecimiento de delitos cibernéticos como la estafa informática.

Integridad de la evidencia electrónica:

La integridad de la evidencia electrónica, según lo descrito por Creswell (2013), implica:

> La salvaguardia de su contenido contra modificaciones no autorizadas o corrupción durante su ciclo de vida. Mantener la integridad de la evidencia es esencial para preservar su valor probatorio y asegurar que los datos digitales presentados en el tribunal reflejen con precisión el estado original de los hechos. (p. 336)

Autenticidad de la evidencia electrónica:

> La autenticidad de la evidencia electrónica se refiere a la verificación de su origen y a la confirmación de que no ha sido objeto de falsificación. Como plantean Denzin, N. K., & Lincoln (2011), esto implica establecer con certeza la identidad de los autores o generadores de documentos electrónicos y verificar que los datos presentados son genuinos y no han sido manipulados o alterados de manera maliciosa. (p. 212)

Cadena de custodia digital:

La cadena de custodia digital, en palabras de Ditton, J., & Short, E. 2019:

> Denota un proceso minuciosamente documentado que registra la posesión, control, transferencia y acceso a la evidencia electrónica desde su recolección inicial hasta su presentación en el tribunal. La preservación de una cadena de custodia sólida es esencial para garantizar la integridad y autenticidad de la evidencia. (p. 89)

Metadatos:

> Los metadatos, conforme a Ditton, J., & Short, E. (2019), son datos que proporcionan información contextual sobre otros datos. En el contexto de la evidencia electrónica, los metadatos pueden incluir detalles como la fecha y hora de creación, modificación y acceso a un archivo digital, lo que es crucial para establecer la autenticidad y la cronología de la evidencia. (p. 159)

Preservación de la evidencia electrónica:

> La preservación de la evidencia electrónica, según Eguzkilore (2006), es el conjunto de procedimientos y políticas destinados a garantizar que la evidencia digital se conserve sin cambios y permanezca disponible para su uso en el proceso legal. Esto implica estrategias como la copia de seguridad de datos, el almacenamiento seguro y la protección contra la pérdida o degradación de la información. (p. 148)

Admisibilidad de la evidencia electrónica:

La admisibilidad de la evidencia electrónica Como señala Pilnik (2017)

> Es el proceso mediante el cual el tribunal evalúa si la evidencia es relevante, confiable y cumple con los estándares legales para ser presentada y considerada durante el juicio. Esta evaluación considera la integridad, autenticidad y cadena de custodia de la evidencia digital. (p. 78)

Estas precisiones terminológicas son vitales para promover una comprensión precisa y una interpretación jurídica adecuada de la evidencia electrónica en el contexto de los casos de estafa informática en la provincia de Córdoba. La claridad en la terminología legal es uno de los pilares de la justicia efectiva en un mundo cada vez más informatizado.

1.7 Conclusiones - Problemas Observados

Teniendo en cuenta las dimensiones de delimitación espacial y temporal establecidas en el marco de este capítulo, el cual se circunscribe al territorio de la provincia de Córdoba, Argentina, y se inserta en el período pos pandémico, se han delineado conclusiones preliminares al término de la revisión bibliográfica y el análisis inicial de la temática.

Dentro de este contexto, se han avistado problemáticas en torno a la administración de la prueba digital en el contexto de los delitos de estafa informática, una problemática de máxima relevancia, materializada en la preservación de la integridad y autenticidad de la evidencia electrónica, cuyos atributos de volatilidad y susceptibilidad a

modificaciones no autorizadas generan inquietudes fundamentales en su tratamiento.

Desde ese punto de vista, resuena la advertencia de Marshall, C., & Rossman, G. B. (2016) acerca de la importancia de mantener la integridad de la evidencia digital a lo largo de su ciclo de vida, salvaguardando su inalterabilidad y veracidad.

Simultáneamente, se constata la carencia de protocolos normalizados y una comprensión insuficiente de la cadena de custodia digital, factores que suscitan preocupaciones sobre la fiabilidad y la idoneidad de la evidencia electrónica presentada en juicio.

Además, se delinean necesidades imperativas en cuanto a capacitación y pericia técnica especializada en la gestión de la evidencia digital, los llamados operadores digitales que intervienen a lo largo de todo el proceso, la interpretación y presentación de esta evidencia exigen competencias altamente especializadas.

La convergencia de estas problemáticas impacta de manera profunda en el ámbito de la justicia penal, con potenciales consecuencias sobre su credibilidad y eficacia, la consecuencia posible de que los perpetradores de delitos cibernéticos eludan la responsabilidad legal debido a los desafíos inherentes a la evidencia digital plantea cuestiones de la máxima envergadura en el marco de la justicia.

La fase consecutiva de este proyecto de investigación, intrínsecamente vinculada a la problematización y búsqueda de soluciones, se erige como una empresa ineludible para avanzar hacia una administración de justicia más eficiente y acorde a las complejidades del contexto actual de los delitos informáticos en la jurisdicción cordobesa.

CAPÍTULO SEGUNDO
MARCO LEGISLATIVO DE LA ESTAFA INFORMATICA Y LA PRUEBA DIGITAL

2. Introducción

Dentro del contexto de la creciente incidencia de la ciberdelincuencia y el papel selecto de la tecnología digital en la comisión de delitos, se presenta el segundo capítulo el cual se adentra en el marco legislativo internacional y nacional que rige los aspectos legales relacionados con la estafa informática y la gestión de pruebas digitales en la provincia de Córdoba.

Este examen es fundamental en un mundo donde las transacciones comerciales y las interacciones sociales han migrado en gran medida al entorno digital, creando un ecosistema propenso a la actividad delictiva en línea (González A., 2018).

Como apunta el destacado experto en delitos cometidos en el ciberespacio, Pilnik (2017), explica

> La prueba digital no solo es una herramienta útil, sino que a menudo es la única fuente confiable de evidencia, por lo tanto, la comprensión de las implicaciones legales y regulatorias que rodean a los delitos cibernéticos y la gestión efectiva de pruebas digitales se han convertido en imperativos en la persecución de la justicia en la era digital. (p. 231)

En este sentido, se exploran los tratados internacionales de relevancia, como el Convenio de Budapest[34] y la Directiva Europea 2013/40/UE[35], que delinean estándares y directrices en la lucha contra la ciberdelincuencia y la protección de datos en línea. Como bien señaló Rodríguez C. (2018), la ciberseguridad y la protección de datos son cuestiones de importancia global, y las normativas internacionales desempeñan un papel vital en la creación de un marco legal coherente para abordar estos desafíos.

Además de lo anterior, se examina la legislación nacional, particularmente la Ley N° 26.388[36], que introduce modificaciones al Código Penal argentino, y se analiza cómo esta normativa impacta en la definición y persecución de la estafa informática. Estas reformas, reflejan los esfuerzos del gobierno argentino por mantenerse al día con las tendencias y desafíos en la esfera cibernética, al tiempo que buscan proporcionar herramientas legales efectivas para abordar los delitos informáticos en el país.

Por último, se aborda el marco legislativo provincial a través del estudio del código de procedimiento penal de la provincia de Córdoba (CPP)[37], destacando su relevancia en la gestión y admisión de pruebas digitales en procesos judiciales. La comprensión de este contexto legal resulta fundamental para la evaluación de la recepción de la prueba digital en casos de estafa informática en la jurisdicción cordobesa y, en última

[34] Es el primer tratado internacional que aborda delitos cibernéticos y la protección de datos en el contexto de las tecnologías de la información y la comunicación (TIC). Fue adoptado en 2001 por el Consejo de Europa y entró en vigor en 2004

[35] Legislación de la UE centrada en armonizar las leyes de los Estados miembros y los ataques contra los sistemas de información - 2013/40/UE

[36] "Ley de Delitos Informáticos". Promulgada el 22 de diciembre de 2008 y se publicó en el Boletín Oficial el 7 de enero de 2009

[37] Ley 8.123, promulgado el 5 de diciembre de 1991 y publicado en el Boletín Oficial el 16 de enero de 1992.

instancia, para el fortalecimiento del sistema de justicia penal en la era digital.

2.1 Legislación internacional

2.1.2 Convenio de Budapest

El Convenio de Budapest, también conocido como el convenio sobre la ciberdelincuencia, consagra un punto de referencia en el ámbito internacional para hacer frente a las complejidades y amenazas asociadas a la ciberdelincuencia en la era digital.

Su adopción en Budapest, Hungría, en el año 2001, representa una respuesta colectiva a la creciente interconexión global y a la consiguiente necesidad de establecer mecanismos efectivos de cooperación entre naciones. Este tratado ha emergido como un cimiento en la lucha contra los delitos informáticos a nivel mundial, destacándose por su enfoque holístico el cual abarca una amplia gama de conductas delictivas digitales.

El espectro de delitos cibernéticos contemplado por el Convenio es vasto e incluye desde la intrusión en sistemas de información y el fraude informático hasta la explotación de la pornografía infantil en línea y la infracción a la propiedad intelectual. Este enfoque integral refleja la comprensión de los desafíos multifacéticos que plantea la ciberdelincuencia y establece un marco normativo que busca adaptarse a la rápida evolución de las tecnologías digitales.

En virtud del convenio de Budapest, los Estados parte[38] tienen la capacidad de colaborar estrechamente en la investigación y persecución de estos delincuentes, compartiendo información crucial sobre la

[38] El 16 de febrero del 2023, Argentina firmó el Segundo Protocolo Adicional, Convención sobre Ciberdelincuencia, conocido mundialmente como el Convención de Budapest

infraestructura empleada y las transacciones de criptomonedas asociadas, facilitando así la identificación y captura de los responsables.

Es crucial destacar que, además de abordar las complejidades técnicas de la ciberdelincuencia, el convenio subraya la importancia de proteger los derechos humanos en el contexto digital, en un entorno global cada vez más interconectado y digitalizado. El acuerdo adquirió una notable relevancia al proporcionar el marco normativo internacional que facilita la armonización legislativa y fomenta la cooperación entre jurisdicciones en la prevención y sanción de la ciberdelincuencia.

Su aplicación en nuestro país y puntualmente en nuestra provincia, se torna esencial para comprender de manera integral el enfoque jurídico en casos de estafa informática y la gestión de pruebas digitales en esta jurisdicción específica.

2.1.3 Tratados internacionales y regionales de cooperación en materia penal

Los tratados internacionales y regionales relacionados con la cooperación en materia de ciberdelincuencia han emergido como respuesta a la creciente proliferación de los delitos informáticos en una era de conectividad global.

Como señala Kaspersky Y. (2010), la naturaleza transfronteriza de la ciberdelincuencia significa que ningún país puede enfrentar eficazmente este desafío por sí solo. Los acuerdos internacionales y regionales buscan llenar este vacío proporcionando un marco legal y operativo para la cooperación entre naciones en la prevención, investigación y persecución de la ciberdelincuencia. En este contexto, el convenio de la OEA sobre ciberdelincuencia ha sido un punto de referencia en América Latina, estableciendo normas y mecanismos para la cooperación en la región.

Un nuevo ejemplo ilustrativo nos basta para dimensionar la importancia de estos tratados; supongamos que necesitamos identificar una red de cibercriminales, los cuales operan en varios países de América Latina, cometiendo defraudaciones de bancas digitales, mediante el uso de un malware. En este escenario, los tratados regionales nos permitirán colaborar y unir esfuerzos entre diferentes países para llevar adelante una investigación conjunta; compartiendo información y asegurando la detención y enjuiciamiento de los ciber criminales. Conjuntamente, estos acuerdos establecen procedimientos claros para la extradición de delincuentes cibernéticos, lo que simplifica su procesamiento legal en el país donde se cometieron los delitos.

En un mundo cada vez más digitalizado, la cooperación internacional en el ámbito de la ciberdelincuencia se ha vuelto esencial para garantizar que los delitos en línea no queden impunes y que se respeten los derechos fundamentales en el proceso (Morales García, O. 2010). E

n el contexto de la provincia de Córdoba y de Argentina, estos tratados influyen en la cooperación internacional y en la gestión de casos de estafa informática y otros delitos cibernéticos cometidos en la región.

Antes de ingresar a desarrollar la legislación nacional en materia de ciberdelincuencia, consideramos fundamental destacar que los tratados internacionales y regionales antes mencionados fomentan la cooperación en materia penal, destacan la relevancia de la ciberseguridad y la necesidad de adaptar el marco legal a la evolución de la tecnología digital y los delitos cibernéticos. Las reformas legales y los tratados internacionales reflejan los esfuerzos de los gobiernos por mantenerse al día con las tendencias y los desafíos en la esfera cibernética, al tiempo que buscan proporcionar herramientas legales efectivas para abordar los delitos informáticos.

Estos desarrollos legales y normativos tienen importantes implicaciones en nuestra provincia y su capacidad para abordar casos de

estafas cometidas en el ciber espacio gestionado evidencia digital, resultan esenciales para su valoración y contribuye al fortalecimiento del sistema de justicia penal.

2.1.4 Directiva Europea 2013/40/UE

La directiva Europea tiene como objetivos fundamentales la inmediación de las normas de derecho penal con todos los casos y variantes de ataques contra los sistemas de información de los estados miembros de la Unión Europea[39]. Esto se logra mediante el establecimiento de normas que delimitan las infracciones penales y las sanciones aplicables, con el propósito de mejorar la cooperación entre las autoridades competentes, incluidas la policía y otros servicios especializados encargados de la aplicación de la ley en los estados miembros, así como organismos especializados de la Unión Europea, como UNODC[40], Eurojust[41], Europol[42] y la ENISA[43].

Los sistemas de información se han convertido en elementos esenciales para la interacción política, social y económica en la Unión Europea. La creciente interdependencia de la sociedad respecto a estos sistemas los convierte en elementos fundamentales para el desarrollo

[39] Asociación política y económica de 27 países europeos que cooperan en una variedad de áreas para promover la paz, la estabilidad y el progreso económico en la región

[40] Oficina de las Naciones Unidas contra la Droga y el Delito (por sus siglas en inglés, United Nations Office on Drugs and Crime).

[41] Agencia de la Unión Europea (UE) establecida para fortalecer la cooperación judicial entre los estados miembros de la UE en la lucha contra la delincuencia transfronteriza y el terrorismo. Creada en 2002 – Con sede en La Haya, Países Bajos.

[42] Oficina europea de policía, es una agencia de la Unión Europea (UE) encargada de mejorar la cooperación y coordinación entre las fuerzas policiales de los Estados miembros de la UE para combatir la delincuencia

[43] Agencia europea de seguridad de las redes y de la información (ENISA, por sus siglas en inglés, European Union Agency for Cybersecurity) agencia de la Unión Europea dedicada a mejorar la ciberseguridad en toda la UE. Fue establecida en 2004 y tiene su sede en Atenas, Grecia.

del mercado interior y la promoción de una economía competitiva e innovadora. En este sentido, la adecuada protección de los sistemas de información se erige como un componente esencial de un marco general efectivo de medidas preventivas que complementan las respuestas del derecho penal frente a la ciberdelincuencia.

En nuestro contexto actual, los ataques contra los sistemas de información, especialmente aquellos vinculados a la delincuencia organizada, representan una amenaza en constante crecimiento a nivel global. La preocupación se intensifica ante la posibilidad de ataques terroristas o de naturaleza política dirigidos a los sistemas de información que forman parte de las infraestructuras críticas de los estados miembros.

Ante esta situación, se hace necesario que la UE responda de manera coordinada y cooperativa a nivel internacional para salvaguardar una sociedad de la información segura y un espacio de libertad, seguridad y justicia.

En la UE, existen infraestructuras críticas cuya perturbación o destrucción tendría repercusiones significativas más allá de las fronteras nacionales, por ello la protección efectiva de estas infraestructuras requiere medidas contra los ataques informáticos respaldadas por sanciones severas que reflejen la gravedad de dichos ataques. La definición de infraestructura crítica[44] abarca elementos, sistemas o partes esenciales para el mantenimiento de funciones vitales en la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población.

La tendencia que se observa a nivel mundial, son ataques de gran escala cada vez más graves y recurrentes contra sistemas de información, los cuales coinciden con el desarrollo de métodos cada vez

[44] Término acuñado por lisainstitute LISA Institute | Oficina Central

más sofisticados, como la creación y utilización de redes infectadas botnets[45]. Estas redes, que pueden activarse sin el conocimiento de los usuarios, representan un grave peligro para el interés público y pueden causar daños colosales e interrumpiendo servicios de los sistemas públicos o generando grandes costos económicos.

La presente directiva se propone establecer sanciones específicas para la fase en la que se crea la red infectada, asegurando la protección ante posibles daños graves, según la legislación y práctica nacionales.

Es esencial destacar que los ciberataques a gran escala pueden ocasionar perjuicios económicos significativos, tanto por la paralización de los sistemas de información y comunicaciones como por la pérdida o alteración de información confidencial de importancia comercial u otros datos.

La Directiva Europea 2013/40/UE, busca una atención especial atención y concientizar a las pequeñas y medianas empresas innovadoras sobre las amenazas vinculadas con tales ataques y su vulnerabilidad, dada su mayor dependencia de los sistemas de información y sus recursos limitados para la seguridad de la información. La cooperación y coordinación internacional se vuelven fundamentales para abordar estos desafíos en el ámbito digital.

Se concluye que esta directiva ha marcado un hito significativo en la concienciación y abordaje de las amenazas cibernéticas, particularmente en el contexto de las pequeñas y medianas empresas. Su enfoque en la cooperación internacional y la sensibilización sobre la importancia de la seguridad de la información ha tenido un impacto significativo en la región del Mercosur, incluyendo el territorio donde se lleva a cabo el presente trabajo de investigación en Córdoba, Argentina.

[45] Red de dispositivos informáticos comprometidos y controlados de manera remota por un actor malintencionado, conocido como "botmaster" o "operador de botnet".

Este impulso regulatorio y de concienciación ha promovido un mayor interés y acción en la protección cibernética, destacando la necesidad de colaboración entre los países vecinos para abordar los desafíos digitales de manera efectiva, integral, para el fortalecimiento de la seguridad de los sistemas de información en toda la región.

a-Entrega y conservación de pruebas electrónicas

Tanto el Consejo de Europa[46] como el Parlamento Europeo[47] han instado a la creación y desarrollo de acciones específicas basadas en un enfoque común de la UE para lograr una asistencia jurídica mutua y más eficaz. Este enfoque busca mejorar la cooperación entre las autoridades de los estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE, así como también poder abordar los desafíos asociados con la determinación y aplicación de la jurisdicción en el ciberespacio.

La Comisión Europea[48] ha optado por regular estas cuestiones a través de un reglamento[49], en lugar de una directiva o decisión, debido a que las órdenes ejecutarán procedimientos transfronterizos, lo que requiere normas uniformes. Esta uniformidad se logra mediante un instrumento en forma de reglamento, garantizando la imposición

46 El Consejo Europeo está compuesto por los jefes de estado o de gobierno de los países miembros de la UE, así como por el Presidente del Consejo Europeo y el Presidente de la Comisión Europea.

47 Una de las principales instituciones de la Unión Europea (UE), junto con el Consejo Europeo, la Comisión Europea, el Tribunal de Justicia de la Unión Europea y el Tribunal de Cuentas.

48 Una de las principales instituciones de la Unión Europea (UE), encargada de ejecutar las políticas y promover los intereses generales de la Unión.

49 Reglamento Del Parlamento Europeo y Del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.

consistente de obligaciones en todos los Estados miembros de la Unión Europea.

La exposición de motivos de la propuesta de reglamento destaca el papel cotidiano de las redes sociales, servicios de correo electrónico, y aplicaciones de mensajería en la comunicación, trabajo y creación de lazos sociales a nivel mundial. Estos servicios, aunque generan beneficios significativos, también pueden ser utilizados para facilitar delitos graves como atentados terroristas. En estos casos, los proveedores de servicios y aplicaciones se convierten en puntos cruciales para la obtención de pruebas e indicios sobre los presuntos autores.

Dada la naturaleza global de las redes sociales, que ofrecen servicios desde cualquier parte del mundo sin necesidad de presencia física y la ausencia de requisitos específicos para la ubicación del almacenamiento de datos, surge la necesidad de abordar la cooperación judicial internacional para acceder a pruebas almacenadas fuera de un país.

El reglamento se enfoca en el desafío procedente de la naturaleza volátil de las pruebas electrónicas y su dimensión internacional, su objetivo es adaptar los mecanismos de cooperación judicial a la era digital. Proporcionando a las autoridades judiciales y policiales las herramientas necesarias para investigar eficazmente el ámbito en el que los delincuentes se comunican en la actualidad.

En este contexto, el instrumento jurídico aborda la necesidad de acceder a datos almacenados fuera del país, por proveedores de servicios ubicados en otros Estados miembros o terceros países, garantizando una respuesta eficiente a las nuevas formas de comunicación delictiva en el entorno digital.

En este sentido, el objetivo principal del reglamento es doble: por un lado, busca fortalecer la seguridad jurídica para las autoridades, proveedores de servicios y personas afectadas, y por el otro, pretende

mantener un nivel uniforme en las solicitudes de las autoridades competentes, todo esto se lleva a cabo sin comprometer la debida protección de los derechos fundamentales, asegurando que cualquier medida solicitada se base en los principios de necesidad y proporcionalidad.

En lo que respecta a la notificación y ejecución de órdenes bajo este instrumento, se establece que las autoridades deben dirigirse al representante legal designado por el proveedor de servicios.

Este enfoque proporciona una solución estandarizada para toda la Unión Europea, permitiendo la transmisión de órdenes a los proveedores de servicios a través de un representante legal. Según lo dispuesto en el artículo 3.7 del reglamento, dicho representante legal debe ser una persona física o jurídica designada por escrito por un proveedor de servicios no establecido en un estado miembro que participe en un instrumento jurídico contemplado en la directiva.

En lo que respecta a las infracciones susceptibles de ser objeto de una orden Europea de conservación, el artículo 5 del reglamento establece que dicha orden puede emitirse para cualquier infracción penal en el estado emisor con una pena máxima de privación de libertad de al menos tres años.

Además, la orden puede aplicarse cuando las infracciones se hayan cometido total o parcialmente a través de un sistema de información, abarcando las infracciones definidas en diversas directivas, tales como:

a) La Directiva (UE) 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo;

b) Infracciones relacionadas con abusos sexuales, explotación sexual de menores y pornografía infantil, conforme a la Directiva 2011/93/UE;

c) Infracciones contempladas en la Directiva 2013/40/UE sobre ataques contra los sistemas de información;

d) Infracciones previstas en la Directiva 2017/541 sobre la lucha contra el terrorismo.

Este enfoque amplio busca abordar distintos ámbitos delictivos y garantizar una respuesta efectiva en casos que involucren sistemas de información, la uniformidad y coherencia en la imposición de obligaciones establecidas por este reglamento han servido como un modelo para promover la armonización de normas y la colaboración en sudamericana.

La experiencia y las lecciones aprendidas por parte de la UE sirven de guía para todos los países del cono sur, para lograr desarrollar políticas y regulaciones que permitan una mayor integración y cooperación regional en la gestión de asuntos transfronterizos y promoviendo el avance hacia un marco regulatorio más sólido y cohesivo en la región.

b-Autoridad competente para la obtención y solicitud de conservación de prueba electrónica

La cuestión de la autoridad competente para emitir órdenes de obtención y conservación de pruebas electrónicas ha generado un intenso debate en la doctrina desde la publicación de la propuesta del reglamento antes mencionado.

Esta propuesta autorizaba tanto a un órgano judicial como a un miembro de la fiscalía a emitir estas órdenes sin diferenciar el tipo de datos y su impacto en los derechos fundamentales del propietario de los mismos.

El dictamen del Comité Económico y Social Europeo(CESE)[50] subrayó la importancia de respetar los derechos fundamentales,

50 Órgano consultivo de la Unión Europea (UE) - establecido en 1957 junto con el Tratado de Roma, que fundó la Comunidad Económica Europea (CEE)-

incluidos los reconocidos en el Convenio Europeo de Derechos Humanos (CEDH)[51] y las Constituciones de los Estados miembros. El CESE argumentó que las solicitudes de obtención de datos de abonados y de acceso pertenecen al ámbito de los derechos de carácter personal, abogando por que las órdenes sean emitidas por una autoridad judicial en lugar de un fiscal.

El Supervisor Europeo de Protección de Datos (EDPS)[52] emitió recomendaciones para que la normativa europea fuera clara, se fortaleciera la seguridad jurídica y se aplicara el principio de proporcionalidad en el listado de infracciones susceptibles de órdenes.

El EDPS expresó preocupación de que el límite de tres años de privación de libertad permitiría solicitar órdenes para casi cualquier delito, sirviendo como un posible coladero para delitos no incluidos en el listado.

En el considerando número 10 del reglamento, se reconoce el respeto por los derechos fundamentales y los principios del CEDH y de los tratados internacionales para la protección de derechos humanos, asegurando la protección de derechos como la libertad y seguridad, la vida privada, la protección de datos personales, la libertad de empresa, el derecho a la propiedad, la tutela judicial efectiva, la presunción de inocencia, el derecho de defensa, y los principios de legalidad y proporcionalidad.

51 Tratado internacional que establece un marco legal para la protección de los derechos humanos y las libertades fundamentales en Europa. Redactado por el Consejo de Europa y firmado en Roma el 4 de noviembre de 1950, entró en vigor el 3 de septiembre de 1953.

52 También conocido como el European Data Protection Supervisor (EDPS), es una autoridad independiente encargada de supervisar y garantizar el cumplimiento de la legislación de protección de datos en las instituciones y organismos de la (UE). Establecido por el Parlamento Europeo y el Consejo de la UE en virtud del Reglamento (UE) 2018/1725 sobre protección de datos en las instituciones de la UE y las normas y políticas relacionadas

Además, el considerando numero 17 establece que el valor probatorio de las pruebas obtenidas bajo el reglamento debe ser evaluado por un juez competente de acuerdo con el derecho nacional.

El artículo 4 del reglamento aborda la autoridad emisora de las órdenes de obtención y conservación de pruebas electrónicas, se establece claramente que la obtención de datos de abonados y de acceso solo puede ser realizada por un juez o fiscal competente y en el caso de datos de tráfico y de contenido. Dispone que solo un órgano judicial puede llevar a cabo la obtención, sin embargo, en la solicitud de conservación de datos, la orden puede ser emitida por un juez, fiscal o cualquier otra autoridad competente actuando como investigador, pero debe ser validada por un juez o fiscal en casos de urgencia.

Ahora bien, en cuanto a la preservación de datos, el reglamento fija un plazo máximo de 60 días, que puede prorrogarse hasta que se emita la orden correspondiente en caso de notificación anticipada. Se ha señalado como una crítica que el texto no establece un periodo limitado para la eliminación de datos en caso de no solicitar su entrega a la autoridad competente, lo que podría plantear problemas en términos de protección de los derechos de los usuarios.

A los fines del presente trabajo, es relevante destacar que el texto final del reglamento parece haber abordado de manera satisfactoria muchas de las preocupaciones planteadas por los estados partes. Asimismo, se observa un esfuerzo por lograr un equilibrio entre la eficacia de la investigación y la protección de los derechos fundamentales en el entorno digital, lo cual es crucial para garantizar una regulación adecuada y respetuosa de los principios democráticos y los valores fundamentales.

Esta mejora y refinamiento del Reglamento puede servir como un ejemplo valioso para la región del Mercosur, proporcionando un marco de referencia para futuras iniciativas regulatorias en temas similares, es que al adoptar un enfoque equilibrado y basado en los derechos

fundamentales, se puede promover una mayor confianza en el entorno digital y fortalecer la protección de los ciudadanos cada vez más digitalizados.

2.2.1 Legislación Nacional - Ley N° 26.388 – Ley Delitos Informáticos y Ciberseguridad

La Ley 26.388, promulgada el 4 de junio de 2008 y publicada en el Boletín Oficial el 25 de junio de 2008, marcó un hito significativo en la incorporación de disposiciones legales relacionadas con los delitos informáticos en el Código Penal de Argentina, esta ley introdujo, a través de su Artículo 9º, el inciso 16, que establece: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos."

Estas enmiendas legales se agruparon bajo el término genérico de "Ley de Delitos Informáticos", su objetivo principal fue incorporar normativas en el marco legal que abordaron las nuevas tecnologías de la información y las comunicaciones que habían surgido a mediados del siglo pasado. Esto se hizo con la intención de superar falencias y lagunas legales que habían surgido a raíz del rápido avance de la tecnología digital, como señala el derecho, como ordenamiento jurídico, siempre se encuentra en una relación de latencia con respecto a los acontecimientos del mundo que observa. Esto, como señala Rosende E. implica que;

> Las normas legales se promulgan después de la observación de los hechos y, en muchos casos, no pueden anticipar eventos futuros que pueden ser inimaginables, este problema se agudiza cuando los cambios en el mundo real no son los hechos en sí, sino la evolución de los medios y las formas en que ocurren estos eventos. (p. 86)

En nuestro país, el desarrollo de la revolución digital fue gradual y no estuvo acompañado por una evolución legislativa adecuada, existieron diversos proyectos de ley que propusieron la inclusión de delitos informáticos en el Código Penal. Sin embargo, estos proyectos legislativos no avanzaron de manera significativa y a menudo quedaron en un estado aislado, estos proyectos abordaron aspectos como el acceso ilegítimo informático, violación de secreto, estafas y otras defraudaciones, daño informático, interrupción de las comunicaciones, delitos que comprometen la paz y dignidad de la Nación, y delitos de propiedad intelectual.

En el año 2006, se presentaron varios proyectos de ley relacionados con delitos informáticos, pero ninguno de ellos fue tratado ni sancionado, lo que llevó a la pérdida de su vigencia legislativa. El proyecto de ley que dio origen a la Ley 26.388 fue el resultado de un esfuerzo conjunto de varios diputados y senadores, y se consolidó como una versión mejorada y refinada de todos los proyectos anteriores (Palazzi, P. A. 2009).

En lo que respecta a la génesis de la Ley 26.388, se ha constatado que esta normativa tuvo su origen en un primer dictamen emitido por las comisiones de comunicaciones e informática y de legislación penal de la cámara de diputados de la nación en el año 2006 (expediente 5864-D-06). Respaldado por la mayoría de los bloques políticos, posteriormente, este proyecto de ley fue sometido a debate en el recinto el 1 de noviembre de 2006, donde la cámara de diputados realizó ciertas modificaciones al texto propuesto por las comisiones, el proyecto luego pasó a la cámara de senadores para su evaluación en las comisiones pertinentes y finalmente fue votado el 28 de noviembre de 2007, incorporando algunas enmiendas adicionales.

En cuanto al contenido del artículo penal en cuestión y motivo de análisis del presente trabajo de investigación, el senado mantuvo la redacción propuesta por la cámara de diputados, con dos exclusiones

específicas, la primera exclusión eliminó la frase "actuando sin autorización del legítimo usuario", considerando que este elemento añadía confusión al tipo penal, ya que la autorización no podría justificar una conducta destinada a defraudar. Mientras que la segunda exclusión eliminó la frase "luego de su procesamiento", ya que no se encontró justificación para fijar un momento técnico específico en una etapa de la transmisión de datos.

Respecto al bien jurídico protegido, es evidente que el objeto resguardado es el patrimonio, no las personas o algún otro derecho, por lo que este enfoque se basa en la interpretación de que, en los casos tratados en esta temática, el patrimonio de la víctima es lo que se ve perjudicado. Dado que el tipo penal es amplio en su alcance, no se ataca directamente la propiedad o algún elemento de propiedad del sujeto pasivo, sino más bien el patrimonio en su conjunto.

La figura delictiva en cuestión, al igual que la defraudación del inciso 15, requiere el cumplimiento de todas las exigencias típicas de cualquier acto de defraudación patrimonial. Sin embargo, se ha establecido que el uso de una técnica de manipulación informática constituye el ardid y el error característicos de este tipo de delitos. Respecto al concepto de "manipulación informática", este hace referencia a la acción de alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones incorrectas o que no se lleven a cabo como se esperaba.

Mientras que la manipulación de datos en sistemas informáticos, se presenta diversas modalidades, una de ellas involucra la inserción de información falsa en una computadora o la alteración de datos una vez que han sido correctamente introducidos en el sistema, e incluso la eliminación de información, en estos casos, no se produce un daño directo, y la conducta se asemeja más a la estafa que al daño informático.

Es importante destacar que la manipulación informática en sí misma no constituye un delito, sino que solo se considera delictiva cuando provoca una alteración en el funcionamiento del sistema informático o la transmisión de datos de la víctima o de un tercero, no se requiere necesariamente que esta manipulación cause un "daño informático" en el sentido del artículo 183, segunda parte, del Código Penal, sino que la alteración del funcionamiento del sistema informático o de la transmisión de datos está relacionada con la propia manipulación.

Consideramos relevante señalar que, a pesar de las críticas que se han planteado sobre la amplitud del tipo penal, como las formuladas por Morales García, O. (2010) en su trabajo titulado "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas".

Es evidente que la delincuencia informática, particularmente en casos de defraudación, puede adoptar diversas formas y evolucionar con rapidez en función de los avances tecnológicos, un enfoque más cerrado en la legislación podría quedar obsoleto en poco tiempo, por lo tanto, la interpretación judicial y doctrinal será fundamental para delimitar el alcance del tipo penal y aplicarlo de manera adecuada a casos en los que se vea afectado el patrimonio de las víctimas.

A pesar de lo hasta aquí expuesto, no se nos escapa el hecho de que la normativa bajo examen no ha eludido críticas, incluyendo la observación de su falta de claridad y la necesidad de realizar interpretaciones extensivas para considerarla congruente con la categoría de conductas fraudulentas, de acuerdo con esta objeción, se aprecia una escasa distinción conceptual en comparación con el delito de hurto, la cual se pretendía diferenciar para resolver las disputas doctrinarias que precedieron a la promulgación de la presente normativa. Consideramos relevante mencionar que se ha cuestionado la viabilidad de esta legislación desde una perspectiva constitucional, dado que su adherencia al principio de estricta legalidad en el ámbito penal,

consagrado en el Artículo 18 de la Constitución Nacional, podría ser objeto de críticas y desafíos sostenidos.

Es importante destacar que el texto de la norma se enfoca en el acto de manipulación sin proporcionar una explicación exhaustiva, lo que sugiere una cierta ambigüedad, la norma alude al acto de manipular, lo cual, por sí solo, no es suficiente para aclarar su alcance, ya que esto conlleva una connotación de actividad prolongada sobre un objeto con la finalidad de obtener algún beneficio.

Es importante señalar que el concepto de perjuicio patrimonial no se encuentra explícitamente definido en la norma, lo que conlleva a que su comprensión se derive de su calidad como delito de defraudación especial y de su ubicación sistemática en el código sustantivo, particularmente en el capítulo dedicado a los delitos contra la propiedad. Además, se plantea la cuestión de por qué el legislador persiste en considerar como acto defraudatorio la apropiación no evidente de un bien ajeno, la norma no brinda una explicación sólida que respalde esta concepción, lo que provoca interrogantes en torno a su capacidad para abordar comportamientos más complejos que los asociados con el hurto convencional.

En cuanto a la aplicabilidad de la norma, se observa que esta se refiere a casos que involucran la manipulación informática con el fin de alterar el funcionamiento normal de un sistema informático o la transmisión de datos, esto significa que no cualquier forma de manipulación informática es relevante, sino solo aquella que pueda tener el potencial de modificar el funcionamiento del sistema en cuestión. La norma es aplicable a cualquier individuo que realice esta manipulación informática con el propósito de obtener un beneficio.

No obstante lo anterior, persiste la crítica de que la norma parece prescindir de la interacción entre el sujeto activo y el pasivo, ya que se hace referencia a "defraudar a otro" sin detallar la participación de ese "otro". Esta falta de interacción se considera esencial en cualquier caso

de defraudación, en cambio, en este supuesto, los actores principales son el sujeto activo y la máquina o sistema informático que es manipulado en beneficio del primero, sin que intervenga en ningún momento la voluntad humana perjudicada en la relación establecida.

Este aspecto unidireccional en la comisión del acto lesivo se asemeja más al acto de apoderamiento, que implica la sumisión de un sujeto a otro, prescindiendo de la voluntad de este último, ya sea para obtener una cosa mediante engaño o para relacionarse de manera lícita en una primera fase y luego defraudar su buena fe.

En cuanto al sujeto activo de este tipo delictivo, puede tratarse de cualquier persona, ya que la normativa se inicia con la expresión "el que", lo que implica que no se requiere ningún estatus especial, inicialmente, este puede ser un mero acto de intrusión en la privacidad de la persona. Pero si el individuo se vale de esta información para cometer un acto fraudulento, la situación evoluciona hacia la ejecución de un delito contra la propiedad, en estos casos, se trata de una conducta de "piratería informática".

En lo que respecta al sujeto pasivo, puede ser cualquier individuo que resulte engañado y sufra un perjuicio patrimonial como consecuencia de la conducta delictiva, así como en el caso del inciso 15°, también es posible que se produzca una estafa en la que intervengan tres partes.

Se ha planteado una crítica en correspondencia a esta formulación, arguyendo que se prescinde de la interacción entre el sujeto activo y el pasivo, a pesar de mencionar "defraudar a otro" sin hacer referencia a la participación de este "otro", esta falta de interacción se considera esencial en cualquier caso de defraudación.

Esta unilateralidad en la comisión del acto lesivo se asemeja más al acto de apoderamiento, que implica la sumisión de un sujeto a otro, prescindiendo de la voluntad de este último, ya sea para obtener una

cosa mediante engaño o para relacionarse de manera lícita en una primera fase y luego defraudar su buena fe.

En lo que respecta al aspecto subjetivo del delito, se considera doloso, con dolo directo, ya que el agente debe conocer y desear la realización de los elementos objetivos del tipo penal.

En cuanto a la consumación y la tentativa, al igual que en otros casos de delitos defraudatorios, la consumación se produce cuando se causa un perjuicio patrimonial como resultado de la utilización de cualquier técnica de manipulación informática que altere el funcionamiento normal de un sistema informático o la transmisión de datos del sujeto pasivo, la tentativa es admisible en este contexto.

2.2.2 Análisis Ley 26.388

El minucioso análisis de la Ley 26.388 y su posterior aplicación en la jurisprudencia revela la existencia de una serie de tensiones y cuestionamientos de índole tanto legal como conceptual. Tal como señala Mendoza, G. (2022), el término "manipulación alterativa" se erige como un desafío interpretativo de considerable envergadura debido a su inherente abstracción, que conlleva la habilidad de englobar una amplia gama de comportamientos informáticos, lo que a su vez dificulta su aplicación precisa.

Según Martínez, R. (2019), la definición de los conceptos de "sistema informático" y "transmisión de datos" asume un papel fundamental en la delimitación de los contornos de esta figura delictiva, suscitando interrogantes acerca de la incorporación de nuevas tecnologías y sistemas emergentes en el ámbito normativo.

En lo que respecta al componente subjetivo de la manipulación informática, la condición de dolo y la exigencia de dolo directo como requisito evidencian la imperiosa necesidad de que el agente tenga conocimiento y voluntad de llevar a cabo los elementos constitutivos del

tipo penal. Como sostiene López, J. (2020), quien insiste respecto a la importancia de comprender la naturaleza de estas conductas en el contexto digital.

Finalmente, la indagación sobre la manipulación informática y su regulación tanto en la ley como en la jurisprudencia, conlleva a una reflexión acerca de la constante adaptación del marco legal ante la evolución tecnológica.

Según Martínez, R. (2019), este proceso debe ser llevado a cabo con el objetivo primordial de mantener un equilibrio equitativo entre la salvaguardia de los derechos individuales y la preservación de la seguridad jurídica.

> La manipulación informática se presenta como un ejemplo paradigmático de cómo el sistema legal debe afrontar los desafíos inherentes a la era digital, planteando cuestiones fundamentales en relación con la interpretación y aplicación de la ley en un mundo cada vez más interconectado y dependiente de la tecnología. (p 81)

2.2.3 Código Procesal Penal de la Nación

La Ley N° 27.063, sancionada en el año 2014, aprobó el Código Procesal Penal de la Nación, posteriormente, la Ley N° 27.482, sancionada en el año 2018, modificó la denominación original del nuevo ordenamiento normativo por la de Código Procesal Penal Federal. Además, dispuso que el Poder Ejecutivo Nacional elaboraría y aprobaría un texto ordenado del Código Procesal Penal Federal, sin introducir modificaciones en su contenido.

Este código presenta numerosos obstáculos en cuanto a la regulación de la evidencia digital, lo cual se refleja en la carencia de normativas específicas que aborden de manera exhaustiva y detallada.

La obtención, presentación y valoración de la evidencia digital en el ámbito judicial, sin embargo algunas disposiciones permiten el uso de medios digitales en circunstancias particulares, esta falta de normativas específicas genera lagunas legales que inciden en la efectividad del enjuiciamiento de delitos informáticos en nuestro país.

Asimismo, el código exhibe carencias normativas específicas en cuanto a la evidencia digital, a pesar de que algunas de sus disposiciones contemplan el empleo de medios digitales bajo circunstancias particulares.

Los medios probatorios establecidos por dicho código incluyen una variedad de modalidades, como audiencias, pericias, inspección judicial, ejecución de planos, reproducciones fotográficas y cinematográficas, entre otros.

Aunque la normativa carece de directrices expresas sobre la evidencia digital, el artículo 206 establece el principio de libertad de la prueba en la investigación penal. La facultad de admisión de medios probatorios, incluida la evidencia digital y equiparándola así a la prueba documental en términos de su consideración y valoración en el proceso judicial. Repárese que el Art. 224. (Párrafo incorporado por art. 5° de la Ley N° 25.760 B.O. 11/8/2003), reconoce el uso de medios electrónicos: En caso de urgencia, cuando medie delegación de la diligencia, la comunicación de la orden a quien se le encomiende el allanamiento podrá realizarse por medios electrónicos. El destinatario de la orden comunicará inmediatamente su recepción al Juez emisor y corroborará que los datos de la orden, referidos en el párrafo anterior, sean correctos. Podrá usarse la firma digital. La Corte Suprema de Justicia de la Nación o el órgano en que ésta delegue dicha facultad, reglamentará los recaudos que deban

adoptarse para asegurar la seriedad, certidumbre y autenticidad del procedimiento.

Sin embargo, las disposiciones no logran abordar de manera exhaustiva la regulación de la evidencia digital y no proporcionan pautas claras sobre su obtención, presentación y valoración en el ámbito judicial, lo que genera incertidumbre y dificultades en el proceso judicial, especialmente en casos relacionados con delitos informáticos.

a-Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos.

La resolución 234/2016, emanada del Ministerio de Seguridad de la República Argentina el siete de junio del 2016, constituyo una de las primeras respuestas gubernamental frente a la creciente amenaza de los ciberdelitos en el contexto de la lucha contra el narcotráfico y el crimen organizado.

Enmarcada en la necesidad de dotar a las fuerzas de seguridad y policiales con las herramientas y conocimientos pertinentes, la resolución refleja el reconocimiento a nivel internacional de la cibercriminalidad como una manifestación intrínseca al crimen organizado. El documento del ministerio destaca la íntima conexión existente entre las TICs y la comisión de delitos, abordando tanto su utilización como medio para perpetrar actos delictivos, como su condición de objeto del delito.

A través de una contextualización legislativa, se hace alusión a las leyes N° 26.388[53] y N° 26.904[54], que establecen el marco normativo para la persecución de ciberdelitos y el delito de grooming, respectivamente.

La resolución subraya la complejidad inherente a la investigación de la delincuencia informática, resaltando la volatilidad y fragilidad de la evidencia digital y la necesidad de su preservación, destaca también lo central de la prueba digital como elemento fundamental para la investigación, reconociéndola como la única evidencia disponible.

La cadena de custodia, la capacitación de las fuerzas de seguridad en la obtención y tratamiento de la evidencia digital, y la colaboración con organizaciones no gubernamentales (ONG) especializadas en la prevención de delitos, son aspectos que se delinean como fundamentales en la resolución.

La aprobación del "Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos" representa el punto central y operativo de esta resolución. Este protocolo establece las pautas y procedimientos específicos que las fuerzas policiales y de seguridad deben seguir durante la investigación y recolección de pruebas en casos de ciberdelitos.

Asimismo, la invitación a las provincias, para adherir al protocolo, tiene como objetivo fomentar una acción coordinada a nivel nacional en la lucha contra el cibercrimen.

---

53 Ley Nacional N° 26.388 de Delitos Informáticos - Sancionada: Junio 4 de 2008 y promulgada de Hecho el 24 Junio del 2008 – ttps://servicios.infoleg.gob.ar/infolegInternet/anexos/140000144999/141790/norma.htm.

54 Ley Nacional N° 26.904 de grooming "acoso sexual de una persona adulta a una niña, un niño o un adolescente por medio de internet." Sancionada: Noviembre 13 de 2013 y promulgada: Diciembre 4 de 2013- https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=223586.

Al promover la adhesión de todas las provincias, se busca garantizar una aplicación uniforme y efectiva de las medidas establecidas en el protocolo en todo el país, lo que contribuirá a mejorar la capacidad de respuesta y la eficacia de las autoridades en la prevención y persecución de los delitos cibernéticos.

b-Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital

La Resolución N° 232/2023 del Ministerio de Seguridad se enmarca en la normativa legal, específicamente la Ley Nº 22.520[55] de Ministerios (Texto Ordenado por Decreto N° 438/92) y sus modificatorias.

La misma confiere al Ministerio de Seguridad la competencia para la determinación de la política criminal y la elaboración de planes y programas a la aplicación de dicha política, se fundamenta en la Ley Nº 24.059[56], que establece las bases jurídicas y funcionales para la seguridad interior, otorgando al Ministro de Seguridad, por delegación del Presidente de la Nación, la facultad de ejercer la conducción política del esfuerzo nacional de policía.

La resolución aludida, destaca la creación del programa de fortalecimiento en ciberseguridad y en investigación del cibercrimen (FORCIC)[57] mediante la Resolución N° 86/22, con el propósito de incrementar las capacidades en la prevención, detección y análisis de incidentes cibernéticos.

55 Boletín Oficial, en vigencia desde el día 22 de diciembre de 1981.

56 Sancionada: Diciembre 18 de 1991, Promulgada: Enero 6 de 1992.

57 Programa de fortalecimiento en ciberseguridad y en investigación del cibercrimen - del 11/2/2022 - BO 15/2/22

En este contexto, la resolución aprobó el "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital"[58], elaborado en colaboración con las fuerzas federales y el Ministerio Público Fiscal.

Este protocolo busca establecer pautas uniformes para la identificación, recolección y preservación de evidencia digital en casos de ciberdelitos, complementando el "Protocolo de actuación para la investigación científica en el lugar del hecho" aprobado previamente.

La medida instruye a las fuerzas policiales y de seguridad federales a implementar el protocolo y extiende la invitación a las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires para adherir al mismo. La entrada en vigor se establece a partir de su publicación en el Boletín Oficial de la República Argentina.

2.4 Legislación Provincial

2.4.1 El axioma de la libertad probatoria en el contexto jurídico y sus restricciones a la luz de las disposiciones constitucionales.

El Código Procesal Penal de la provincia de Córdoba (CPPC)[59] establece en su artículo 192 el "principio de libertad probatoria", este principio, tal como lo describe Cafferata Nores (2012), confiere la facultad de emplear cualquier medio de prueba con el propósito de corroborar los eventos y circunstancias relacionados directamente con el objeto del proceso.

Sin embargo, es fundamental tener en cuenta que, como apunta el autor, las limitaciones inherentes al principio de libertad probatoria son igualmente importantes para asegurar la equidad y la legalidad del

58 Se adjunta en la sección "ANEXO" del presente trabajo final.

59 Ley 8.123. Cordoba, 5 de Diciembre de 1991 Boletín Oficial, 16 de Enero de 1992

proceso y no pueden admitirse medios probatorios que menoscaben la moral, que estén expresamente prohibidos (como lo establece la Constitución Provincial en el artículo 41 en el caso de cartas o documentos privados sustraídos), o que sean incompatibles con el sistema procesal o el ordenamiento jurídico vigente.

Además, se restringen aquellos medios que condicionen el derecho del imputado a observar una actitud defensiva pasiva en el proceso, el principio de libertad probatoria. Debe considerarse en conjunto con las importantes restricciones y limitaciones del derecho procesal penal, a fin de garantizar un equilibrio entre la obtención de pruebas y la protección de los derechos fundamentales de las partes involucradas en el proceso penal.

En el análisis de las limitaciones relacionadas con la aplicación del principio de libertad probatoria, se puede concluir que la admisibilidad de la prueba en un proceso penal y su capacidad para ser efectiva en la formulación de un juicio condenatorio dependen en gran medida de su conformidad con el sistema procesal y el marco legal vigente. Como destacan Cafferata Nores (2012) y Mendoza (2022) en sus respectivas obras, el respeto por las normas y las garantías constitucionales desempeña un papel central en la promoción de la justicia y la salvaguarda del debido proceso en cualquier sistema jurídico.

En este contexto, cabe mencionar que las garantías constitucionales, como el derecho a la presunción de inocencia, que establece que toda persona es inocente hasta que se demuestre su culpabilidad, desempeñan un papel crucial. El respeto por esta presunción es esencial para asegurar que las pruebas presentadas en el proceso no socaven la presunción de inocencia del imputado.

Por su parte, el derecho a un juicio justo, que incluye la imparcialidad del proceso y la igualdad de armas entre la acusación y la defensa, es otro aspecto vital que debe ser observado. También, del respeto por el derecho a la inviolabilidad de la conciencia, que prohíbe la

obtención de pruebas mediante coerción directa, física o psicológica, con el fin de forzar a las personas a proporcionar información o pruebas, constituye un pilar fundamental para garantizar la integridad del proceso.

Por último, la salvaguardia del derecho a la privacidad y la prohibición de la obtención de pruebas mediante tortura o tratos inhumanos o degradantes subrayan la importancia de que las pruebas en el proceso penal sean congruentes con el marco legal y respeten los derechos fundamentales de todas las partes involucradas. Es de suma importancia reconocer que la efectividad de las pruebas en un proceso penal depende directamente de su conformidad con las garantías constitucionales y el marco jurídico, lo que a su vez garantiza la equidad y el respeto por los derechos fundamentales de todas las partes en el proceso legal.

En el contexto de este trabajo final de tesis, resulta necesario reconocer la importancia de las garantías constitucionales, las cuales establecen un marco fundamental para el adecuado desarrollo de procesos legales, aunque no profundizaremos en el alcance de estas garantías, es pertinente hacer una breve evocación de las mismas como punto de partida para los párrafos subsiguientes.

En la cima de nuestra jerarquía normativa, se destaca el artículo 18 de la Constitución Nacional (CN), el cual ocupa una posición preeminente y fundamental en el ordenamiento legal de nuestro país, el mismo confiere una serie de garantías esenciales. Entre las que se encuentra la inviolabilidad de la defensa en juicio de la persona y de los derechos, la inviolabilidad del domicilio, de la correspondencia epistolar y los papeles privados.

Es importante destacar que esta garantía viene acompañada de una disposición que estipula que "una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación" (Baigún, D., & Zaffaroni, E. 2004).

Además, este mismo artículo establece la prohibición de penar a cualquier habitante de la Nación sin un juicio previo fundado en una ley anterior al hecho del proceso, este último aspecto consagra el principio del "nullum crimen, nulla poena sin lege" o "principio de legalidad", de esta premisa se derivan diversas garantías, incluida la garantía jurisdiccional que exige que la existencia del delito y la pena a imponer sean determinadas mediante una sentencia judicial y un procedimiento legalmente establecido.

Estas mismas garantías están reconocidas en numerosos pactos internacionales que han adquirido rango constitucional en virtud de la reforma de 1994, como se dispone en el artículo 75, inciso 22 de la CN, por otra parte, el artículo 19 de la CN consagra el principio de la privacidad, otorgando una sólida protección a la esfera íntima de las personas.

Estas disposiciones constitucionales, desempeñan un papel fundamental en la preservación de los derechos y libertades. Tal como señala Mensa González, A (2020) la Constitución de la provincia de Córdoba, en particular, el artículo 40 de la CP Córdoba garantiza la inviolabilidad de la defensa, el artículo 45 protege la inviolabilidad del domicilio, y el artículo 46 establece

> El secreto de los papeles privados, la correspondencia epistolar y cualquier otra forma de comunicación personal, por cualquier medio que sea, es inviolable. La ley determina los casos en que se pueden proceder al examen o interceptación mediante orden judicial debidamente motivada. (p. 14)

Estas disposiciones, tanto a nivel nacional como provincial, constituyen cimientos sólidos para el respeto de los derechos y garantías individuales en el marco de los procesos legales y la protección de la privacidad de los ciudadanos.

La aplicación del principio de libertad probatoria en el contexto del proceso penal, a pesar de su importancia en la búsqueda de la verdad, no es absoluto, sino que se halla sujeto a restricciones de relevancia significativa.

El empleo de cualquier medio de prueba debe ajustarse estrictamente al respeto de cada una de las garantías constitucionales consagradas en nuestra Carta Magna, mediante disposiciones constitucionales, como aquella que asegura la inviolabilidad del domicilio (artículo 18), o la que proclama que "las acciones privadas de los hombres (...) están exentas de la autoridad de los magistrados" (artículo 19), se han delineado esferas de privacidad protegidas contra una injerencia estatal indiscriminada.

De igual manera, la Constitución Nacional ha declarado como inviolables "la defensa en juicio de la persona y de los derechos", lo cual comprende el derecho de que el Estado respete aquellos ámbitos de privacidad sobre los cuales los titulares han manifestado un interés legítimo en que se mantengan intactos, en el marco de la evolución tecnológica y la creciente interacción de las personas en los entornos digitales.

Resulta fundamental reconocer que el principio de libertad probatoria en el proceso penal no puede menoscabar las garantías constitucionales que salvaguardan la privacidad y la intimidad de los individuos, estableciendo así un equilibrio entre la búsqueda de la verdad y la protección de los derechos fundamentales (Mendoza, G., 2022).

Es incuestionable que los entornos digitales y las nuevas formas de comunicación, en los cuales diariamente interactuamos y en los que depositamos y registramos aspectos íntimos y privados de nuestra vida, constituyen ámbitos que merecen una salvaguardia efectiva contra cualquier intromisión estatal. En este contexto, es importante recordar la existencia de los derechos constitucionales no enumerados, reconocidos en el artículo 33 de la Constitución Nacional (CN).

Según lo enfatiza Mendoza G. (2022), los ámbitos de privacidad no enumerados expresamente por la Constitución, como es el caso de los entornos digitales, para obtener reconocimiento como tal, deben cumplir con dos requisitos fundamentales.

En primer lugar, que el individuo haya demostrado, a través de su conducta, un interés en mantenerlo en privado. En segundo lugar, que tal expectativa de privacidad sea considerada razonable por parte del Estado, como ilustra el autor mencionado; "una conversación telefónica, sin importar su contenido, genera una expectativa razonable de que solo estamos siendo escuchados por nuestro interlocutor y no por un grupo de agentes de policía que comentan sobre nuestra actividad, gustos y preferencias" (Mendoza, G. , 2022).

Los entornos digitales albergan esferas de privacidad profundamente arraigadas en la vida de las personas, y cualquier interferencia estatal que busque obtener elementos probatorios en este contexto debe cumplir con requisitos estrictos.

En este sentido, dicha intromisión debe estar debidamente fundamentada, ser ordenada por una autoridad jurisdiccional en el marco de una causa penal previamente iniciada y contar con elementos objetivos que respalden la necesidad de llevar a cabo dicha acción. Montas L. (2016) subraya que

> Estas injerencias solo pueden justificarse cuando existen razones de sospecha suficientemente sólidas que respalden la creencia de que, en el contexto de un proceso penal, existen motivos suficientes que justifiquen la búsqueda de pruebas en el ámbito de los entornos digitales, los entornos digitales constituyen áreas de privacidad significativa para las personas, y cualquier intento estatal de obtener pruebas en estos entornos debe cumplir con requisitos

estrictos y ser respaldado por una base sólida de sospechas en el contexto de un proceso penal, de manera que se protejan tanto la privacidad individual como el debido proceso. (p. 257)

Sin lugar a dudas, es imperativo contar con una legislación que establezca las condiciones y los procedimientos bajo los cuales el Estado puede intervenir en el ámbito de la privacidad digital con el propósito de obtener elementos probatorios para esclarecer un delito.

El marco normativo que rige el proceso penal en la provincia de Córdoba reconoce el principio de libertad probatoria, pero este principio no puede eludir las limitaciones constitucionales que deben ser respetadas por los mecanismos de obtención de pruebas y las medidas de coerción para ser considerados válidos y efectivos.

Hasta la fecha de la elaboración del presente trabajo de investigación, no existe una regulación clara y precisa que establezca directrices para la adquisición, el manejo y la incorporación al proceso de pruebas digitales.

Dada la significativa intrusión estatal que implica el acceso al contenido de dispositivos como teléfonos móviles o computadoras, la intervención en comunicaciones digitales o la revisión de registros de comunicaciones anteriores de un usuario de telefonía, se torna imperiosa la necesidad de promulgar una legislación específica y dejar de aplicar figuras legales análogas.

En este contexto, cabe citar las palabras de López, J., quien destaca:

> Es importante recordar que la intimidad se relaciona con un espacio de libertad donde la personalidad y el proyecto de vida se desarrollan sin interferencias externas, este espacio abarca la elección de comunicarse con ciertas personas, sobre ciertos contenidos y a

través de determinados medios. La intimidad también genera expectativas de confidencialidad y, en cualquier caso, implica el derecho a excluir a otros de su conocimiento. (pp. 45-64)

Solo una ley debe determinar en qué circunstancias y con qué justificaciones se permite su conocimiento y acceso.

Resulta esencial establecer una regulación legal que respete la privacidad y que defina los procedimientos y condiciones bajo los cuales el Estado puede acceder a pruebas digitales.

Esta regulación debe ser cuidadosa y garantizar la protección de los derechos fundamentales y la intimidad de las personas, ya que la intrusión en este ámbito debe ser rigurosamente regulada para equilibrar la búsqueda de la verdad y la protección de la privacidad.

2.4.2 Acuerdos reglamentarios de Tecnologías Informáticas en la Provincia De Córdoba

El máximo tribunal de nuestra provincia ha demostrado un compromiso continuo con la modernización y eficiencia en la administración de justicia a través de la adopción progresiva de tecnologías informáticas.

A título ejemplificativo, se destaca el acuerdo reglamentario Nº 882, Serie "A", de fecha 17/05/07, que estableció la firma digital para sentencias y autos en los juzgados de ejecución fiscal de la ciudad de Córdoba. Asimismo, el acuerdo reglamentario Nº 1319, Serie "A", del 01/12/15, introdujo el sistema de apertura y consulta de saldos de cuentas judiciales en el banco de la provincia de Córdoba, junto con el sistema de orden de pago electrónica, actualmente en pleno funcionamiento en todo el ámbito del poder judicial de la Provincia de Córdoba.

Otros acuerdos significativos incluyen el Nº 1103, serie "A", de fecha 27/06/12, que marcó el inicio de la utilización de cédula de notificación digital, y el acuerdo reglamentario Nº 1494, serie "A", del 21/05/18, que abordó la implementación de oficios electrónicos.

Finalmente, el acuerdo N° 1582 de expediente judicial electrónico refleja la cooperación entre el Tribunal Superior de Justicia, la federación de colegios de abogados de Córdoba y el colegio de abogados de la ciudad de Córdoba, el mismo busca perfeccionar el servicio de administración de justicia, la digitalización de datos, documentos y procedimientos, como también la introducción de firmas digitales y electrónicas, conforme a normativas nacionales y provinciales.

Estos reglamentos establecen hitos y procedimientos esenciales en la tramitación de causas judiciales y propone la ampliación del alcance de acuerdos relacionados con notificaciones electrónicas y el uso de protocolos electrónicos de sentencias o autos. El acuerdo también refleja el compromiso conjunto de las entidades judiciales para modernizar y agilizar los procesos judiciales a través de la implementación de tecnologías y prácticas eficientes.

2.5 Conclusiones - Problemas Observados

Las conclusiones de este capítulo arrojan luz sobre una serie de observaciones cruciales en el contexto de la relevancia de la prueba digital en el delito de estafa informática en la provincia de Córdoba.

En primer lugar, es evidente que la legislación internacional y regional, como el convenio de Budapest y la directiva Europea 2013/40/UE, desempeña un papel esencial en la cooperación internacional y la armonización de leyes en la lucha contra la ciberdelincuencia. Estos acuerdos proporcionan un marco sólido para abordar la complejidad de los delitos cibernéticos y garantizar que los delincuentes no puedan evadir la justicia al cruzar fronteras (Morales

García .O, 2010). Su influencia se refleja en la legislación nacional y provincial de la provincia de Córdoba, lo que afecta directamente a la gestión de pruebas digitales y la persecución de la estafa informática en la región.

En segundo lugar, y a modo de alerta, es crucial destacar que la provincia de Córdoba carece de protocolos, acuerdos reglamentarios o guías específicas para la recolección de evidencia digital. La ausencia de pautas claras y estandarizadas para la recolección de evidencia digital puede dar lugar a inconsistencias en los procedimientos, lo que a su vez podría comprometer la integridad de las pruebas y socavar la validez de los procesos judiciales relacionados con delitos cibernéticos. Por lo tanto, es imperativo que se implementen medidas concretas para abordar esta brecha normativa y garantizar una gestión adecuada de la evidencia digital en nuestra provincia.

En el próximo capítulo, se examinarán casos concretos, examinados directamente desde la fuente jurisprudencial y se analizará cómo estos marcos legales impactan en la práctica y en la administración de justicia en el contexto de la ciberdelincuencia en Córdoba.

CAPÍTULO TERCERO
MARCO JURISPRUDENCIAL DE LA ESTAFA INFORMÁTICA Y LA PRUEBA DIGITAL

3. Introducción

Este capítulo aborda de manera exhaustiva el marco jurisprudencial relativo a la admisión e incorporación de la prueba digital en el contexto del proceso penal en el ámbito de las estafas informáticas.

En un contexto caracterizado por una creciente digitalización, se funda este análisis como una pieza fundamental para la comprensión de las complejidades inherentes a la incorporación de la evidencia digital en el ámbito legal, la estructura del capítulo se articula en torno a varios ejes temáticos trascendentales.

Primero, se examinará con detenimiento el marco jurídico y jurisprudencial de la provincia de Córdoba, Argentina, con el fin de identificar los enfoques y prácticas específicas en esta región. A continuación, se amplía la perspectiva al ámbito todo el territorio argentino, lo que permite un análisis más amplio de las tendencias y enfoques nacionales en relación con la admisión y evaluación de pruebas digitales en casos de estafas informáticas. Adicionalmente, se considera la jurisprudencia de otras provincias argentinas, lo que proporciona un contexto comparativo para evaluar la consistencia o variabilidad en la aplicación de la ley en diversas regiones del país.

Asimismo, se investiga la intersección precisa entre las estafas informáticas y las pruebas digitales en la provincia de Córdoba, examinando cómo se han manejado los casos reales en esta jurisdicción y los desafíos que han surgido en la admisión de pruebas digitales en el marco de los procesos penales, para así dar vida a la investigación y poder contextualizarla.

A lo largo del capítulo se presentarán casos reales e ilustrativos que ejemplifican diversas modalidades de estafas informáticas y el

manejo de la evidencia digital recolectada en el caso específico, estos ejemplos proporcionan una visión práctica y aplicada de los conceptos teóricos y jurisprudenciales.

Finalmente, se sintetizan las conclusiones clave y se resaltan los problemas observados en la admisión y valoración de pruebas digitales en casos de estafas informáticas, estableciendo así las bases para una comprensión más profunda de los retos que enfrenta el sistema legal en la era digital.

3.1 Análisis jurisprudencial relativo a la admisión e incorporación de la prueba digital en el proceso penal

Esta investigación se enfoca en una exhaustiva revisión jurisprudencial acerca de la admisión e integración de la prueba digital en el contexto del proceso penal provincial y nacional. Este análisis se configura como un componente esencial para comprender las complejidades intrínsecas de la evidencia digital en el ámbito legal.

Para llevar a cabo este examen, se procederá a identificar y analizar criterios específicos empleados por diversos tribunales de nuestro país, en cuanto a la aceptación de pruebas digitales, destacando ejemplos paradigmáticos de fallos que han sentado precedentes significativos.

Además, se abordarán los desafíos y controversias recurrentes en la incorporación de evidencia digital, examinando casos emblemáticos que hayan suscitado debates respecto a la autenticidad y la integridad de dicha evidencia.

Este análisis no solo busca proporcionar una visión general de la evolución jurisprudencial en respuesta a los avances tecnológicos, sino también brindar una comprensión más profunda de la aplicación práctica de los principios jurídicos en la era digital, contribuyendo así al acervo de conocimientos jurídicos en el ámbito del derecho procesal penal.

3.2 Marco Jurídico y Jurisprudencial de Córdoba:

3.2.1 Fallo reseñado: "Quipildor, Armando Andrés p. S. A. Coacción calificada, grooming, producción de material de abuso sexual de menores de 18 años, etc." (Expte. SAC n° 8934647).

El fallo referido destaca la importancia de la evidencia digital, específicamente aquella almacenada en la web, en el marco de un caso en el que se investiga la comisión de diversos delitos a través de medios digitales. El tribunal enfoca su atención en el riesgo potencial que representa la liberación del imputado para la integridad de esta evidencia.

El argumento central se fundamenta en la premisa de que la mayoría, o posiblemente la totalidad, de la evidencia crucial está bajo la custodia de la fiscalía, asimismo el tribunal expone la preocupación de que, en caso de libertad del imputado, exista un elevado riesgo de que pueda en libertad, manipular, alterar o incluso eliminar de dicha evidencia. Este riesgo se fundamenta en la capacidad del acusado para acceder a dispositivos con conexión a internet, desde los cuales podría influir en la información almacenada.

El fallo resalta la magnitud del riesgo al mencionar la presencia de numerosos hechos, víctimas y damnificadas cuyas imágenes e información personal están resguardadas en los dispositivos del imputado. Además, el fallo insiste en que estas imágenes y datos aún no han sido identificados ni declarados por la fiscalía, lo que refuerza la importancia de preservar la integridad de la evidencia digital.

Esta sentencia destaca la relevancia de la gestión y preservación adecuada de la evidencia digital en casos judiciales, reconociendo la necesidad de previsiones cuando la misma se encuentra almacenada en

línea (también llamado "en la nube")[60] y puede ser accesible para el imputado. La decisión del tribunal se fundamenta en la preocupación legítima de evitar la posible alteración de pruebas cruciales para el caso.

3.2.2 Fallo reseñado: "Banco de la provincia de Córdoba / Rivera, Vanesa Yanina presentación múltiple – abreviados" (Expte. N° 5926974)".

La sentencia analizada aborda la disputa legal entre el Banco de la Provincia de Córdoba S.A. y Vanesa Yanina Rivera, focalizándose en la restitución de veinticinco mil pesos ($25,000) y otros conceptos, originados por un presunto préstamo solicitado por la demandada mediante cajero automático ATM.

La Cámara 7ª en lo Civil y Comercial de Córdoba respaldó la decisión de primera instancia que desestimó la demanda del banco, esta resolución destaca que el crédito "preaprobado" obtenido mediante un cajero automático no fue solicitado por Rivera, sino por un tercero que canalizó los fondos a su cuenta. El fallo enfatiza la aplicación de normas de derecho al consumidor, subrayando la responsabilidad del banco como proveedor de servicios para prevenir ciberestafas.

En el contexto de la presentación del BPC, que buscaba la restitución de fondos basándose en una supuesta solicitud de préstamo por parte de Rivera. Esta última refutó las alegaciones, arguyendo ser víctima de una maniobra defraudatoria ejecutada por un tercero, Rivera sostenía que proporcionó su cuenta a su tío sin conocer la ulterior transferencia no autorizada y la solicitud del préstamo.

La cámara, respaldada por el dictamen de la Fiscalía Civil, determinó que el acto carecía de validez para configurar una relación

60 Proceso de guardar datos de manera remota en servidores en línea, en lugar de hacerlo en dispositivos de almacenamiento físico como discos duros o unidades USB.

jurídica válida debido a vicios y defectos genéticos, asimismo se enfatizó que la demandada no tenía la intención de solicitar el préstamo y que fue un tercero quien ejecutó la solicitud.

En cuanto a la evidencia digital, la sentencia reconoció la existencia de un hecho delictivo en la causa penal "Di Leo Horacio p. s. a. Defraudación Informática, etc. (Expte. N° 2062815)", donde se declaró al imputado responsable de defraudación mediante manipulación informática, este dictamen respaldo la afirmación de Rivera de ser víctima de una maniobra defraudatoria por parte de un tercero.

El tribunal evaluó el deber de seguridad del banco como proveedor, especialmente en el contexto de créditos preaprobados, concluyendo que el Banco de Córdoba no demostró haber tomado medidas adecuadas para evitar el riesgo de ciberestafas.

Este fallo subrayó la obligación de la entidad de otorgar al cliente la misma seguridad que existiría en transacciones realizadas a través de un cajero humano. En consecuencia, la sentencia sostuvo que, al verificarse el incumplimiento del deber de seguridad establecido en la Ley de Defensa al Consumidor (Ley Nº 24.240)[61], el Banco debe asumir los resultados financieras perjudiciales, sin poder reclamar a la cliente la restitución de los fondos desembolsados en contravención de la obligación de seguridad que la entidad estaba obligada a cumplir.

La cámara rechazó la apelación presentada por el Banco de la Provincia de Córdoba SA, respaldando el dictamen de la Fiscalía, y considerando la evidencia digital como un elemento clave para establecer la veracidad de los hechos en el contexto de ciberestafas.

61 Normas de Protección y Defensa los Consumidores, Sancionada: Setiembre 22 de 1993, Promulgada Parcialmente: Octubre 13 de 1993.

3.2.3 Fallo reseñado: Sala Penal - Tribunal Superior - Sentencias N° 203 - Año: 2020 "Carignano, Franco Daniel p.s.a. producción de imágenes pornográficas de menores de 18 años, etc. -recurso de casación-" (SAC 2469171).

El caso aborda la producción de imágenes pornográficas de menores de 18 años y plantea cuestiones fundamentales relativas a la correcta aplicación de disposiciones legales y la fundamentación de la pena impuesta a Carignano.

En el contexto del análisis, se destaca la relevancia de las tecnologías de la información y comunicación (TIC), las cuales desempeñaron un papel central en los delitos imputados a Carignano. La actuación del imputado se caracterizó por la utilización de las TIC, como las redes sociales, para ocultar su identidad y llevar a cabo un plan delictivo dirigido a atentar contra la integridad sexual de las víctimas.

La naturaleza delictiva de Carignano se inscribe en un marco societal transformado por las TIC, donde la interacción en el ciberespacio propicia la comisión de delitos con características particulares. El uso coactivo de las TIC, el anonimato que brindan y la capacidad de lesión a distintos bienes jurídicos son aspectos que emergen como consecuencias directas de la "era digital".

El tribunal resalta que, a pesar de la falta de contacto corporal físico directo, el delito imputado implica un verdadero acto de abuso sexual, la distancia física se ve trascendida por la capacidad de las TIC para facilitar la coacción y la obtención de imágenes impúdicas.

En el caso, las coacciones ejercidas a través de las redes sociales llevaron a una calificación legal de abuso sexual gravemente ultrajante, resaltando cómo las leyes deben adaptarse y considerar los avances tecnológicos para abordar de manera efectiva los delitos cometidos en entornos virtuales.

El fallo subraya la importancia de adaptar la interpretación legal a la nueva realidad generada por la tecnología, reconociendo que las TIC han expandido los horizontes del delito y presentan riesgos distintos que deben ser abordados en el ámbito judicial.

3.3 Ámbito nacional.

3.3.1 Fallo reseñado: "Camara nacional criminal y correccional Federal - La sala sexta causa N° 39779, "G. R. Y otro s/procesamiento", RTA. EL 3/8/2010"

El fallo descripto resulta ser el primer procesamiento por el delito de phishing en Argentina, el mismo explora con detenimiento tanto los elementos sustanciales del delito como las consideraciones vinculadas a la evidencia digital, marcando así un hito en la jurisprudencia relacionada con fraudes informáticos.

En la imputación, se centra la atención en las maniobras de fraude llevadas a cabo mediante la técnica de manipulación informática conocida como phishing, los acusados lograron obtener datos; como el código de transferencia y el número de tarjeta de crédito, a través de la creación de una página duplicada lo que posteriormente les permitió realizar transferencias fraudulentas desde la cuenta bancaria de la víctima.

Este caso adquirió relevancia no solo por la tipificación del delito en el artículo 173, inciso 16, del Código Penal, sino también por el análisis pormenorizado de la evidencia digital asociada al phishing.

El fallo destacó la necesidad de preservar la integridad de la evidencia electrónica, subrayando que su manipulación inadecuada podría comprometer su validez y, por ende, la solidez del caso presentado.

El fallo estableció precedentes esenciales en la conceptualización y persecución del phishing, reconociendo la creación de una página falsa

como una forma específica de manipulación informática. Igualmente, resaltó la importancia de considerar la evidencia digital de manera meticulosa en casos de fraude informático, haciendo hincapié en la necesidad de adoptar medidas específicas para recolectar, preservar y analizar esta forma de prueba.

El primer fallo en materia de estafa informática nos brinda una plataforma para la exploración detallada de las implicancias legales y técnicas relacionadas con delitos informáticos, la manipulación informática y la evidencia digital emergen como áreas críticas de estudio, subrayando la complejidad y la intersección entre la tecnología y el derecho en la era digital.

En este sentido, la sentencia contribuye al corpus jurídico y académico sobre delitos cibernéticos, estableciendo un marco conceptual y normativo para abordar casos similares en el futuro.

3.3.2 Fallo Reseñado: ”Tribunal: Cámara federal de casación penal, casación penal - Sala IV- fecha: 22/03/2013 partes: Gil, Juan José Luis s/ref. de casación”.

En la sentencia del Tribunal Oral en lo Criminal Federal de Santa Fe, el imputado J. J. L. G. fue condenado por los delitos de amenazas agravadas y coacciones agravadas, relacionados con el envío de correos electrónicos amenazantes de forma anónima, la defensa interpuso un recurso de casación, cuestionando la validez de la prueba informática obtenida en el domicilio del imputado.

Además de lo anterior, la defensa argumentó que la notebook secuestrada no fue adecuadamente resguardada, exponiéndola a posibles contaminaciones, y que no se mantuvo la cadena de custodia de manera adecuada. Puntualizando deficiencias en la pericia informática, como la falta de fajado en los puertos de alimentación

eléctrica y la realización del peritaje en una provincia diferente a la del secuestro.

En relación con la materialidad de los hechos, la defensa cuestionó la existencia de uno de los correos electrónicos y la ubicación desde la cual se envió el otro. También se argumentó que la cuenta de correo involucrada había sido utilizada desde diferentes ubicaciones y por varias personas, lo que socavaría su fiabilidad como prueba incriminatoria.

Asimismo, la defensa destacó que las presuntas víctimas recibieron los correos electrónicos a través de reenvíos, y cuestionó la veracidad de los testimonios de algunos testigos. Se argumentó que la posesión de copias de la causa por parte del imputado no debería considerarse como elemento incriminatorio, ya que otras personas también tenían acceso a dicha documentación.

En su dictamen, el fiscal general solicitó el rechazo del recurso de casación, respaldando la validez de la prueba informática y la conclusión del tribunal respecto a la materialidad de los hechos. Por su parte el análisis que realizó el tribunal de casación destacó la adecuada documentación del secuestro y aseguramiento de la notebook, la continuidad de la cadena de custodia y la realización del peritaje sobre copias del equipo, preservando la integridad del contenido original.

El fallo enfatizó la importancia de adoptar precauciones especiales en la manipulación de evidencia digital, resulta relevante destacar que el tribunal de casación respaldó la decisión previa, subrayando toda la documentación secuestrada y el aseguramiento de la notebook.

La continuidad de la cadena de custodia fue clave, al igual que la realización del peritaje sobre copias del equipo, lo que aseguró la preservación del contenido original. En este contexto, se resaltó la importancia de adoptar precauciones especiales en el manejo de la evidencia digital para evitar su alteración, daño o destrucción.

El fallo destaca la necesidad de cumplir con estándares rigurosos en la recolección, preservación y examen de evidencia electrónica, reconociendo su susceptibilidad a manipulación y la importancia de su integridad en el proceso penal.

La defensa, al no lograr desvirtuar eficazmente los procedimientos seguidos, no logró invalidar la prueba informática. Este caso sirve como antecedente para remarcar la complejidad inherente a la gestión de evidencia digital en el ámbito jurídico y destaca la importancia de seguir buenas prácticas para garantizar su validez y utilidad en el proceso judicial.

3.3.3 Fallo reseñado: "Causa nº 25.405/2021 (reg. Interno del TOCC 15 nº 7155) Lucas Alberto Dodero P.SA. delito de defraudación mediante una técnica informática. - Poder judicial de la Nación tribunal oral en lo criminal y correccional nro. 15"

El fallo referido aborda el supuesto en el que se acusó a Dodero por el delito de defraudación, específicamente en correspondencia al uso de una aplicación bancaria abierta en el teléfono móvil de la víctima.

Debemos tener en cuenta que el art. 172 del Código Penal establece el delito de defraudación como la acción de engañar a otro mediante el uso de un nombre falso, identidad simulada, títulos falsos, influencia ficticia, abuso de confianza o la apariencia de poseer bienes, crédito, comisión, empresa o negocio, o utilizando cualquier otro ardid o engaño.

Además de lo anterior, el art.173 inc. 16 del Código Penal considera un supuesto especial de defraudación, que implica el uso de cualquier técnica de manipulación informática que altere el funcionamiento normal de un sistema informático o la transmisión de datos.

En este caso, el tribunal determinó que los hechos no se ajustaban al tipo penal de la defraudación mediante técnica de manipulación informática, ya que no hubo una interferencia directa en el sistema informático del banco o de una plataforma asociada que alterara los mecanismos de seguridad o modificara los datos.

En cambio, se plantea la posibilidad de considerar si la conducta del acusado en el uso no autorizado de la aplicación bancaria se ajustaría al artículo 173 inc.15 del Código Penal, el cual establece como delito, el uso de una tarjeta de compra, crédito o débito que haya sido falsificada, adulterada, robada, perdida u obtenida del emisor legítimo mediante engaño, o mediante el uso no autorizado de sus datos.

Sin embargo, el tribunal también señaló que, en el caso, no se había logrado acreditar el elemento subjetivo en relación con el acusado antes de cometer la defraudación. En otras palabras, no se había logrado demostrar que el acusado haya participado previamente en un plan para proporcionar la cuenta a la cual se transferiría el dinero antes de solicitar el préstamo.

Dado que este aspecto subjetivo no se había conseguido, el tribunal concluyó que no es posible emitir una condena de acuerdo con la solicitud del Ministerio Público Fiscal (MPF), especialmente porque el MPF no presentó pruebas sustanciales para respaldar esta parte de la acusación.

El fallo plantea la posibilidad de que, en caso contrario, los hechos acreditados podrían ser considerados como un delito de encubrimiento y menciona la existencia de un proceso anterior en el que el tribunal consideró esta posibilidad. El fallo sugiere que se llevarán a cabo análisis adicionales en todo lo que atañe al desarrollo de la materia.

Una correcta incorporación de pruebas digitales desempeña un papel fundamental en el proceso penal, ya que puede ser determinante para alcanzar una sentencia condenatoria en lugar de una absolución.

Este proceso implica no solo la obtención y presentación de evidencia digital, sino también garantizar su autenticidad, integridad y relevancia.

Los tribunales deben ser capaces de evaluar de manera rigurosa y justa las pruebas digitales, considerando su admisibilidad y su peso en el contexto del caso. Resulta crucial que se respeten los principios legales fundamentales, como el principio "in dubio pro reo", que establece que en caso de duda, se debe favorecer al acusado.

En este contexto, la incorporación adecuada de pruebas digitales no solo fortalece la lucha contra la impunidad, sino que también garantiza la protección de los derechos fundamentales de los acusados en el proceso penal.

3.4 Jurisprudencia de otras provincias.

3.4.1 Fallo reseñado: "Cámara de apelaciones en lo penal, penal juvenil, contravencional y de faltas de la ciudad autónoma de buenos aires, SALA III - s/ estafa informática - 12/09/2022".

Con relación a la jurisprudencia mencionada, se destaca que la correcta calificación legal en casos de defraudación informática requiere una consideración minuciosa de los elementos involucrados, incluyendo la adecuada incorporación de pruebas digitales.

La mera utilización de una red informática o el ingreso a un sistema con datos de acceso sin autorización no es suficiente para subsumir una conducta en el tipo penal de defraudación informática.

En su lugar, el tipo penal exige que se utilicen técnicas que efectivamente alteren el normal funcionamiento del sistema informático o la transmisión de dato.

En este contexto, es fundamental analizar los hechos concretos del caso para determinar si hubo una manipulación de datos o si la víctima proporcionó los datos de acceso de forma voluntaria, la correcta

presentación y evaluación de pruebas digitales desempeñan un papel crucial en esta determinación.

En el caso en cuestión, la evidencia sugiere que el acusado obtuvo los datos legítimos de acceso de la víctima a través de engaño, sin necesidad de manipular el sistema de home banking.

Además, es relevante considerar la jurisdicción y la transferencia de competencias en relación con los tipos penales en cuestión. La competencia de los tipos penales previstos en el inc. 16 del art. 173 del Código Penal y en el art.172 del mismo cuerpo normativo no ha sido transferida a la justicia de la Ciudad Autónoma de Buenos Aires, según las leyes correspondientes.

Por último, es importante señalar que el recurso interpuesto por la fiscalía podría haber sido rechazado desde un principio, ya que fue presentado por un fiscal auxiliar sin una delegación adecuada ni justificación de la falta de participación de la fiscal titular.

Contraviniendo procedimientos legales y constitucionales, estos elementos subrayan la importancia de una sólida fundamentación, procedimientos legales adecuados y la correcta incorporación de pruebas digitales para asegurar una correcta calificación legal en casos de defraudación informática y, en última instancia, alcanzar una sentencia justa y equitativa.

3.4.2 Fallo reseñado: "P. L. M. A. c/ Menchini Hermanos S.A. s/ Cobro de pesos Tribunal: Juzgado en lo civil, comercial y minas de San Luis Sala / Juzgado / Circunscripción / Nominación - Fecha: 25 de septiembre de 2023".

La sentencia emitida por el Juzgado en lo Civil, Comercial y Minas de San Luis el 25 de septiembre de 2023, el cual, a pesar de no

encontrarse firme, resalta la trascendental función del código hash en la evaluación de la evidencia digital en el contexto jurídico.

En el fallo, se enfatiza que el código hash, al permanecer inalterado desde el momento de la incorporación de la prueba hasta la realización de la pericia informática, desempeña un papel fundamental para garantizar la autenticidad e integridad de la evidencia.

Este concepto se erige como un pilar esencial para validar la fecha de creación, el contenido y el autor de archivos digitales, proporcionando así una sólida base para la toma de decisiones judiciales. El fallo destaca la importancia de este resguardo en el contexto laboral, donde la evidencia digital puede ser determinante, como se evidencia en casos de despido con causa, subrayando la necesidad de una adecuada preservación y verificación de la cadena de custodia de dicha evidencia en el ámbito legal.

El código hash, en el ámbito de la informática, se configura como un valor alfanumérico de longitud fija, obtenido mediante la aplicación de un algoritmo de función hash a un conjunto específico de datos, como archivos o mensajes, esta huella digital única. También conocida como resumen, posee características fundamentales, tales como su longitud constante, su irreversibilidad, que impide la regeneración de los datos originales a partir del hash, y su eficiencia en el cálculo, incluso para conjuntos extensos de información.

Además, se busca una distribución uniforme, asegurando que conjuntos diferentes de datos generen códigos hash distintos, en el ámbito de la evidencia digital, el código hash desempeña un papel crucial, ya que su utilización permite verificar la autenticidad e integridad de archivos digitales, proporcionando una herramienta esencial para asegurar que no hayan sido objeto de modificaciones no autorizadas.

Este componente tecnológico se erige como una salvaguarda significativa en la seguridad informática y la preservación de la integridad de la información en entornos digitales.

3.5 Jurisprudencia de Estafa Informática y Prueba Digital: Análisis Multifacético

El examen exhaustivo de fallos provenientes de diversos tribunales revela una serie de problemas intrínsecos en la aplicación jurisprudencial en los casos donde debe valorarse la prueba digital.

El problema destacado y tal como lo desarrolla Gómez, A. (2018), se vincula con la correcta presentación y evaluación de pruebas digitales, la complejidad inherente a las tecnologías involucradas y la falta de estándares claros para la admisión de evidencia digital han generado discrepancias en la valoración de la misma.

La calidad y autenticidad de la evidencia digital, esencial para establecer la culpabilidad o inocencia del acusado, a menudo dependen de la pericia técnica y la presentación adecuada en el tribunal, lo que subraya la necesidad de protocolos estandarizados (González, S. 2017).

En última instancia, estos problemas observados destacan la urgencia de abordar las lagunas y ambigüedades en la jurisprudencia relacionada con la prueba digital.

La consolidación de criterios uniformes en la interpretación de elementos legales clave y la implementación de estándares claros para la presentación y evaluación de pruebas digitales son imperativos para garantizar la coherencia y la equidad en el sistema legal en el contexto de la creciente digitalización de las transacciones y delitos.

En cuanto al delito de estafa informática, uno de los desafíos fundamentales identificados radica en la interpretación y aplicación

consistente de los elementos específicos que configuran el delito de defraudación informática.

Adicionalmente, se observa una disparidad en la interpretación del elemento subjetivo del acusado antes de cometer la defraudación, la ausencia de una demostración concluyente de la participación previa del acusado en un plan para la transferencia de fondos antes de solicitar el préstamo ha sido un punto de discordia y la necesidad de establecer claramente la intención del acusado y la ausencia de criterios uniformes para su evaluación plantean interrogantes en torno a la consistencia de la jurisprudencia.

Conclusiones

El análisis jurisprudencial en el ámbito de la estafa informática y la prueba digital revela la complejidad inherente a la calificación legal de estos casos en el contexto jurídico de Argentina, desde el examen detallado de fallos en la provincia de Córdoba hasta la consideración de jurisprudencia nacional y de otras provincias. Se evidencia la necesidad de una evaluación meticulosa de los elementos involucrados en casos de defraudación informática.

En el fallo de la provincia de Córdoba, específicamente en el caso de Dodero, el tribunal destacó la importancia de acreditar el elemento subjetivo del acusado antes de la comisión del delito.

La falta de pruebas sustanciales para respaldar esta parte de la acusación llevó a la conclusión de que no era posible emitir una condena, este fallo subraya la importancia de una presentación completa y sólida de pruebas para respaldar las acusaciones de defraudación informática.

En conclusión, el análisis jurisprudencial desarrollado, nos lleva a acentuar la necesidad de una sólida fundamentación, procedimientos legales adecuados y la correcta incorporación de pruebas digitales para asegurar una correcta calificación legal en casos de defraudación

informática y, en última instancia, alcanzar una sentencia justa y equitativa, estos aspectos son esenciales en el marco legal argentino, especialmente en un entorno legal cada vez más digitalizado.

CAPÍTULO CUARTO

LA INCORPORACIÓN DE PRUEBA DIGITAL EN EL PROCESO PENAL.

4. Introducción

Este capítulo propone ahondar en los medios de prueba tradicionales y en la evolución de la prueba digital, destacando cómo la tecnología ha permeado las actividades cotidianas, generando una nueva categoría de pruebas con su propio conjunto de desafíos y requisitos.

Se examinarán los principios probatorios aplicables a este fenómeno, considerando tanto su continuidad con los principios establecidos como las adaptaciones necesarias para abordar la singularidad de la prueba digital.

Asimismo, se explorarán los principios específicos que rigen la prueba digital, como la integridad de la evidencia, la autenticación y la preservación de la cadena de custodia, reconociendo la necesidad de adaptar las prácticas judiciales a la era digital.

En este contexto, la protección de garantías constitucionales, la obtención legítima de prueba y la posible afectación de la privacidad serán temas centrales de análisis, considerando la delicada intersección entre el avance tecnológico y los derechos individuales.

En última instancia, este capítulo se propone arrojar luz sobre la complejidad y las implicaciones de la incorporación de prueba digital en el proceso penal, subrayando la necesidad de un equilibrio entre la eficacia probatoria y la protección de derechos fundamentales en la era digital.

4.1 La incorporación de prueba digital en el proceso penal.

La incorporación adecuada de pruebas digitales en el proceso penal requiere una sólida comprensión de las técnicas involucradas, es fundamental garantizar la autenticidad, integridad y admisibilidad de estas pruebas, así como proteger la privacidad y los derechos fundamentales de las partes involucradas.

Esto puede implicar la colaboración entre profesionales del derecho y expertos en tecnología forense para garantizar que las pruebas informáticas sean recopiladas de manera legal y forensemente válida.

Además, resulta útil destacar que todas las partes del proceso (jueces, abogados, asesores, fiscales, etc) se encuentren adecuadamente capacitados en cuestiones relacionadas con la evidencia digital para poder evaluar y utilizar estas pruebas de manera efectiva en el proceso judicial. La incorporación de este tipo de pruebas es un aspecto crucial en la modernización del sistema judicial y requiere una combinación de conocimientos técnicos y legales, así como la implementación de protocolos y procedimientos adecuados para garantizar la integridad y la justicia en el uso de estas pruebas en los tribunales.

4.2 Medios de prueba

Los medios de prueba constituyen los elementos sustantivos empleados para acreditar o desvirtuar la existencia de hechos pertinentes en un procedimiento judicial (Palazzi, 2016).

Estos medios desempeñan una función primordial en el proceso legal al respaldar las alegaciones de las partes involucradas y servir como fundamento para las determinaciones judiciales, la clasificación de los medios de prueba abarca diversas categorías. Entre las que se destacan:

La prueba testimonial, que implica los testimonios orales de testigos bajo juramento. La prueba documental, que comprende documentos escritos, impresos o electrónicos que presentan información relevante. La prueba pericial, que incorpora opiniones de expertos en áreas técnicas o científicas (Ebert & Maurer, 2017). La prueba material o real, que refiere a objetos tangibles y evidencia física. La prueba audiovisual, que incluye grabaciones de audio o video; y las presunciones y ficciones jurídicas, que se basan en inferencias lógicas cuando la evidencia directa es insuficiente (Bossler, 2018).

La admisibilidad y valor probatorio de estos medios están sujetos a normas y procedimientos legales. El tribunal, en su función de evaluación, considera la pertinencia y credibilidad al tomar decisiones (Pérez, 2022).

La correcta presentación y gestión de los medios de prueba son aspectos cruciales en la conducción efectiva de un proceso judicial, destacando la importancia de salvaguardar los principios de equidad y justicia procesal (Maimon,D., & Hunt, D. E., 2020).

Ahora bien, este panorama refleja la complejidad y vitalidad de los medios probatorios en el ámbito jurídico, constituyendo un aspecto fundamental en la formación de juicio de los operadores jurídicos y la administración de justicia.

4.3 Aspectos de la prueba. Actividad probatoria. Libertad probatoria

En el ámbito jurídico, la prueba constituye un elemento fundamental en el ámbito judicial, siendo sus aspectos inherentes elementos cruciales para la determinación de la verdad en el proceso legal.

Los aspectos de la prueba engloban características esenciales, tales como la pertinencia, la adhesión a las reglas procesales, la

credibilidad y la relevancia de la evidencia presentada, todos ellos determinantes para la idoneidad probatoria (González, 2017).

La actividad probatoria, por su parte, representa el conjunto de acciones llevadas a cabo por las partes intervinientes en el proceso, dirigidas a recopilar, presentar y evaluar pruebas mediante diversos medios, como testimonios, documentos y peritajes, con el objetivo de respaldar sus alegaciones.

En este contexto y siguiendo la obra de Sánchez, M.

> La libertad probatoria se erige como un principio que confiere a las partes la facultad de seleccionar y presentar evidencia de manera autónoma, siempre y cuando se ajusten a los preceptos legales establecidos, permitiendo así la adaptación de la actividad probatoria a las particularidades de cada caso con miras a la consecución del debido proceso legal y la búsqueda de la verdad jurídica. (pp. 78-96)

4.3.1 Naturaleza y características de la prueba digital

La prueba digital, es la evidencia electrónica derivada de datos generados, almacenados o transmitidos por dispositivos electrónicos (Pérez, 2022).

Esta categoría de prueba abarca una amplia gama de información, que incluye correos electrónicos, archivos digitales, registros de transacciones y metadatos. Estos datos pueden ser generados tanto de manera activa por los usuarios como de forma pasiva mediante registros automáticos de sistemas.

La autenticidad e integridad de este tipo de pruebas digitales, así como su susceptibilidad a posibles manipulaciones, requieren una atención especial en lo que respecta a la cadena de custodia, extracción

y preservación, mediante la implementación de procedimientos específicos.

Es imperativo garantizar una correcta incorporación de estas pruebas al proceso penal, para ello, es fundamental contar con conocimientos especializados en aspectos como la recuperación de datos, el análisis forense digital y la ciberseguridad. Estos conocimientos se convierten en requisitos fundamentales para asegurar el correcto desarrollo del proceso judicial (Martínez, 2019).

La variabilidad de las regulaciones y normativas a nivel jurisdiccional, así como el respeto a la privacidad y derechos individuales, conforman elementos esenciales a considerar en la utilización de prueba digital. La admisibilidad de esta forma de evidencia en el tribunal se enfrenta a nuevos desafíos, requiriendo la observancia rigurosa de estándares legales para asegurar su validez y fiabilidad.

La incorporación de la prueba informática dentro del marco de un proceso judicial es de aquellas cuestiones que conllevan una trascendencia significativa tanto como su grado de dificultad para obtenerla, dadas las características ínsitas que trae aparejado este tipo de pruebas, las cuales son muy específicas.

La prueba informática tiene por objeto cualquier registro que pueda ser generado dentro de un sistema informático, entendiendo por éste, a todo dispositivo físico (computadoras, smartphone, tablets, CDs, DVD, pen drives, etc.) o lógico. Empleado para crear, generar, enviar, recibir, procesar, remitir o guardar a dichos registros, que, producto de la intervención humana u otra semejante, ha sido extraída de un medio informático. Por ejemplo: registros en planillas de cálculo, correos electrónicos, registros de navegación por Internet, bases de datos, documentos electrónicos, etc.

Una de las particularidades de la prueba informática es que puede ser manipulable mediante la intervención humana, por ende, susceptible

de sufrir desde alteraciones hasta su supresión inclusive. Cabe distinguir la prueba informática en atención a esas características específicas: es constante, pues los registros informáticos se hallan resguardados en soportes físicos como ser, por ejemplo, los discos duros de las computadoras o CD-ROM, etc. y aquella que es volátil, porque el registro (la información) está contenido en almacenamientos temporales, tales como memoria RAM, memoria caché o la memoria de dispositivos (por ejemplo en placas de red y placas de video).

4.3.2 Evidencia física vs evidencia digital

La distinción entre evidencia física y evidencia digital emerge como un componente esencial en la evaluación y presentación de pruebas en el ámbito jurídico (Palazzi, 2016).

La evidencia física, comprendiendo elementos tangibles perceptibles por los sentidos como documentos impresos, objetos y muestras biológicas, contrasta con la evidencia digital, conformada por datos almacenados electrónicamente, incluyendo archivos digitales, correos electrónicos, metadatos y otra información procesable por sistemas informáticos.

La evidencia física, por su tangibilidad, se expone a problemáticas como deterioro, contaminación o pérdida, subrayando la imperativa necesidad de una cadena de custodia adecuada para salvaguardar la integridad y autenticidad de dicha evidencia.

Por otro lado, la evidencia digital, al carecer de tangibilidad, plantea desafíos adicionales relacionados con la autenticidad, integridad y susceptibilidad a manipulación, resaltando la necesidad de emplear técnicas especializadas y rigurosos protocolos evidencia (Mason, 2010).

La incursión de la evidencia digital en el ámbito jurídico no solo presenta oportunidades, sino también desafíos sustanciales (Maimon & Hunt, 2020).

Debemos tener siempre presente que la naturaleza dinámica y maleable de la información digital engendra dificultades específicas en cuanto a su autenticidad y preservación, la amenaza de manipulación, la rápida obsolescencia de tecnologías y la variabilidad en los estándares de seguridad digital son retos que requieren una atención minuciosa.

En el ámbito de los códigos procesales vigentes en nuestro país, se constata la ausencia de una delimitación explícita del concepto de evidencia digital. Ante esta carencia normativa, resulta pertinente recurrir a fuentes internacionales especializadas para establecer parámetros definitorios sólidos.

En este contexto, el reglamento general de protección de datos (RGPD)[62] de la Unión Europea para fuerzas y cuerpos de seguridad, jueces y fiscales emerge como una referencia relevante, conforme surge de dicha guía, la evidencia digital se conceptualiza como "aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial" (Consejo de Europa, 2009).

Este enfoque normativo europeo proporciona una base conceptual robusta para abordar la evidencia digital en el ámbito del derecho procesal penal. Integrando así por principios que reconocen la importancia de la información generada electrónicamente y su pertinencia en el contexto jurídico.

La adopción de esta definición contribuye a llenar el vacío normativo existente, alineando la jurisprudencia regional con estándares internacionales en materia de prueba electrónica y ofreciendo una plataforma conceptual coherente para la aplicación de estos principios en los procedimientos judiciales.

62 Reglamento de la Unión Europea que entró en vigencia el 25 de mayo de 2018, establece un marco legal para la protección de datos personales de los ciudadanos de la UE y del Espacio Económico Europeo

Asimismo la jurisprudencia y normativa legal han evolucionado para abordar estos desafíos, estableciendo estándares y procedimientos específicos dirigidos a la admisión y evaluación adecuada de la evidencia digital.

La adaptación constante prácticas delictivas y avances tecnológicos agrega un estrato adicional de complejidad, requiriendo una actualización constante de estrategias forenses y protocolos legales para enfrentar nuevos escenarios y amenazas emergentes en el ámbito de la evidencia digital (Bossler, 2018).

Especial mención merece la norma ISO/IEC 27.037:2012[63], sobre la gestión de evidencia digital, la norma propone directrices fundamentales para su tratamiento. Destacando la necesidad de adherirse a métodos específicos que salvaguarden, la originalidad de la prueba y permitan, en la medida de lo posible, la obtención de copias de respaldo.

Asimismo, la norma aboga por la instauración de un proceso auditable, donde los procedimientos y la documentación generada deben ajustarse a las buenas prácticas profesionales. Este enfoque garantiza la trazabilidad del trabajo desempeñado, posibilitando el seguimiento preciso de los procesos y sus resultados.

Además, la N-ISO/IEC 27.037:2012 enfatiza sobre la importancia de un proceso reproducible. El cual requiere que la evidencia sea obtenida de manera que los métodos y procedimientos empleados sean reproducibles, verificables y argumentables.

63 Estándar internacional que proporciona directrices para la identificación, adquisición, preservación y presentación de evidencia digital en el contexto de investigaciones forenses. Fue desarrollado conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Este criterio facilita que otros expertos puedan validar las actuaciones realizadas, promoviendo la transparencia y confiabilidad en el manejo de la evidencia digital.

Adicionalmente, la normativa aboga por la instauración de un proceso defendible, donde se precisa la identificación y validación de las herramientas utilizadas en el análisis de evidencia digital, estas herramientas deben ser nombradas, validadas y contrastadas específicamente para el propósito previsto en el análisis, fortaleciendo así la robustez y credibilidad del proceso.

4.4 Cadena de Custodia

La gestión de la cadena de custodia para la evidencia digital se convierte en un proceso aún más crucial debido a la complejidad inherente y a los desafíos específicos asociados con la naturaleza intangible de la información electrónica (Palazzi, 2009).

A medida que la tecnología avanza, la gestión y preservación de la cadena de custodia para la evidencia digital se vuelve más compleja y demanda una atención meticulosa (Pérez, 2022).

Uno de los desafíos principales radica en la volatilidad de los datos digitales, que pueden ser fácilmente modificados, alterados o borrados sin dejar rastro visible (Bossler, 2018; Ebert & Maurer, 2017).

La constante evolución de las tecnologías y la diversidad de formatos de datos presentes en dispositivos electrónicos requieren protocolos especializados para garantizar la recopilación y preservación adecuada de la evidencia.

Además, la necesidad de mantener la integridad técnica de la evidencia digital resalta la importancia de documentar minuciosamente cada paso del proceso, desde la adquisición hasta la presentación en el tribunal.

La cadena de custodia para evidencia digital también enfrenta desafíos relacionados con la autenticidad y la seguridad de los datos almacenados (Maimon & Hunt, 2020).

La posibilidad de manipulación o intrusiones durante la recolección y el análisis de evidencia digital subraya la necesidad de contar con profesionales capacitados en ciberseguridad forense y la implementación de medidas de seguridad robustas.

La diversidad de dispositivos y plataformas digitales, así como la rápida obsolescencia tecnológica, generan dificultades adicionales para mantener la cadena de custodia (Ebert & Maurer, 2017).

La actualización constante de protocolos y prácticas es esencial para adaptarse a los cambios en el panorama tecnológico y abordar nuevos desafíos emergentes, la cadena de custodia de evidencia digital presenta desafíos significativos debido a la complejidad tecnológica y la naturaleza dinámica de los datos electrónicos.

La implementación exitosa de protocolos especializados y la capacitación continua del personal son elementos fundamentales para asegurar la integridad y la admisibilidad de la evidencia digital en un entorno legal en constante evolución.

Dada la complejidad y dinámica de la tecnología, contar con profesionales debidamente capacitados en ciberseguridad forense se convierte en un requisito imperativo, la actualización constante de los conocimientos y habilidades del personal encargado de manejar la evidencia digital es esencial para adaptarse a las nuevas amenazas y desafíos emergentes en el ámbito de la ciberseguridad.

La implementación de protocolos especializados se erige como uno de los objetivos centrales del presente ensayo académico. Respaldados por la correspondiente normativa legal y las mejores prácticas en el campo.

Estos protocolos abordaran no solo los aspectos técnicos de la gestión de la evidencia, sino también aspectos éticos y legales, asegurando la integridad y autenticidad de la información a lo largo de la cadena de custodia.

La inversión en la formación continua del personal y la actualización de los protocolos se posiciona como una estrategia proactiva para enfrentar los desafíos cambiantes de la evidencia digital. Sumado a la colaboración entre profesionales del derecho, expertos en ciberseguridad y tecnólogos resulta crucial para desarrollar e implementar protocolos que no solo cumplan con los estándares actuales, sino que también se anticipen a futuros avances tecnológicos y desafíos en el ámbito de la ciberseguridad.

La integridad del proceso judicial y la confianza en la validez de la evidencia digital dependen, en última instancia, de una implementación diligente de protocolos especializados y una formación continua que garantice la competencia y actualización constante del personal involucrado.

4.5 Categorización del rastro

La categorización del rastro digital constituye un proceso esencial en la gestión de la evidencia digital en el ámbito jurídico.

Este procedimiento implica la clasificación y organización sistemática de la información recopilada, permitiendo una comprensión estructurada de los elementos probatorios relevantes para una investigación (Ebert & Maurer, 2017).

La categorización del rastro digital involucra la identificación de patrones, conexiones y relaciones entre datos electrónicos, con el propósito de establecer la relevancia y coherencia de la evidencia en el contexto de un caso judicial. Este enfoque contribuye a una presentación

ordenada y comprensible de la información ante las instancias judiciales, facilitando la toma de decisiones informadas.

La adecuada categorización del rastro digital, respaldada por protocolos especializados y el conocimiento técnico, se posiciona como un componente crucial para fortalecer la solidez y credibilidad de la evidencia digital en el proceso legal.

La aplicación de estos protocolos no solo asegura la coherencia en la clasificación de la evidencia, sino que también respalda la autenticidad y la integridad de los datos a lo largo de la cadena de custodia (Maimon & Hunt, 2020).

En última instancia, la categorización efectiva del rastro digital contribuye significativamente a la construcción de argumentos sólidos y a la toma de decisiones judiciales fundadas en el contexto de investigaciones relacionadas con la evidencia digital (Ebert & Maurer, 2017).

4.6 Principios probatorios aplicables

En el ámbito en el cual nos encontramos inmersos, la gestión de pruebas se rige por principios probatorios fundamentales que garantizan la validez y confiabilidad de la evidencia presentada en un proceso legal.

Estos principios, resultan esenciales y son la columna vertebral del debido proceso y la administración de justicia, aplicables tanto a la evidencia física como a la evidencia digital.

Uno de los principios fundamentales es el de legalidad, que establece que, toda prueba presentada debe ser obtenida de conformidad con la ley y respetar los derechos y garantías de las partes involucradas (Cafferata Nores, 2012).

Además, se aplica al principio de pertinencia, que exige que la evidencia sea relevante para los hechos en cuestión y contribuya a la resolución de la controversia (Davara Rodríguez, 1997).

En el contexto del presente trabajo, recalcamos el principio de autenticidad, el cual requiere demostrar que la información electrónica presentada es lo que se afirma ser y que no ha sido manipulada. Asimismo, este principio exige que la evidencia digital se encuentre completa y sin alteraciones desde su obtención hasta su presentación en el proceso judicial.

La cadena de custodia, es otro principio esencial, el mismo asegura la trazabilidad y la preservación adecuada de la evidencia desde su recolección hasta su presentación en el tribunal, garantizando su admisión como prueba válida.

Además, el principio de contradicción permite a las partes cuestionar y contradecir la evidencia presentada, asegurando un debate justo y equitativo (Donna, 2001).

Estos principios probatorios son cruciales para mantener la integridad del proceso judicial y garantizar la confianza en la justicia. Se observa que la aplicabilidad de estos principios tanto a la evidencia física como a la digital refleja la necesidad de adaptar los estándares jurídicos a los avances tecnológicos en la era digital.

Se recalca, que la adaptación de estos principios probatorios a la era digital es crucial para abordar los desafíos específicos asociados a los tiempos que corren.

Nuevamente destacamos la necesidad de desarrollar marcos legales y normativas actualizadas para garantizar que la justicia sea efectiva, confiable y en constante evolución.

4.6.1 Principios específicos de la prueba digital

A los fines del presente trabajo final, es necesario abordar los principios específicos que se desprenden del ámbito probatorio. Estos principios tienen en cuenta las particularidades de la evidencia electrónica y buscan asegurar su validez y confiabilidad en el marco de un proceso legal.

Integridad Digital: Este principio establece que la evidencia digital debe mantener su integridad a lo largo de su ciclo de vida, desde la obtención hasta su presentación en el tribunal, buscando prevenir cualquier alteración o manipulación de la información electrónica (Martínez, 2019).

Tridimensionalidad: Implica considerar no solo el contenido visible, sino también los metadatos, elementos coligados que pueden ser relevantes para la comprensión y autenticidad de la prueba (González, 2018).

Cadena de Custodia Digital: Se centra en asegurar la trazabilidad y seguridad de la evidencia electrónica a lo largo de su procesamiento, almacenamiento y presentación en el proceso judicial (Pérez, 2022).

Habilidad Técnica: Este principio reconoce la importancia de la competencia técnica y especializada de los profesionales encargados de manejar la evidencia digital, se busca garantizar que las personas involucradas en la recolección y presentación de la prueba posean el conocimiento necesario para preservar su autenticidad[64].

Normativa Actualizada: Este principio enfatiza la necesidad de seguir normativas y estándares actualizados en la gestión de la evidencia digital. La adaptación constante a los cambios tecnológicos es esencial para mantener la confiabilidad de la prueba (Ebert & Maurer, 2017).

64 Temática abordada en profundidad en el siguiente capítulo, en el apartado de la responsabilidad de los diferentes operadores

4.6.2 Protección de las garantías constitucionales

La protección de las garantías constitucionales es esencial para salvaguardar los derechos fundamentales de las personas involucradas en un proceso legal.

a- Obtención Legítima de Prueba

La legitimidad en la obtención de la prueba digital es crucial para garantizar su validez y adhesión a los derechos constitucionales, se debe demostrar que la recolección de la evidencia ha seguido protocolos legales y respetado los derechos individuales, evitando prácticas ilegítimas o violatorias de la privacidad (Donna, 2001).

b- Afectación de la Privacidad – Fundamento Constitucional

El uso de pruebas digitales en el marco de un proceso judicial plantea desafíos que deben ser abordados con un sustento constitucional sólido, a fin de garantizar el respeto a los derechos y garantías fundamentales de los ciudadanos.

En este sentido, es indispensable tener en cuenta los principios consagrados en nuestra Constitución y tratados internacionales con jerarquía constitucional, particularmente en lo referido a los derechos a la privacidad, el debido proceso y las garantías procesales.

En primer lugar, el art. 19 de la Constitución Nacional establece el principio de intimidad, protegiendo a las personas de injerencias arbitrarias en su vida privada. La obtención y utilización de pruebas digitales debe estar sujeta a un escrutinio estricto para garantizar que no se vulneren estos derechos.

Tal como lo indica la Corte Suprema de Justicia de la Nación, toda intervención en la privacidad debe ser legítima, necesaria y proporcional, respetando el ámbito de reserva de los individuos.

Asimismo, el art 18 de la Constitución Nacional, en su referencia al debido proceso, subraya que "ningún habitante de la Nación puede ser penado sin juicio previo". Este principio asegura que cualquier prueba, incluida la prueba digital, debe ser obtenida y presentada de manera lícita, garantizando siempre el derecho a la defensa en juicio.

En consonancia con este precepto, la recolección de pruebas digitales debe ajustarse a los principios de legalidad y contradicción, como bien lo establecen la jurisprudencia y la doctrina argentina. Lo que significa que las partes involucradas deben tener pleno acceso a la evidencia presentada, así como la oportunidad de cuestionarla adecuadamente.

El derecho a la privacidad también encuentra amparo en tratados internacionales como la Convención Americana sobre Derechos Humanos[65], que en su art. 11 consagra el derecho a la honra y a la dignidad, protegiendo a las personas de intromisiones arbitrarias o abusivas en su vida privada.

A su vez, el art. 8 del mismo pacto garantiza el derecho a un debido proceso, el cual incluye la igualdad de armas y el acceso pleno a la evidencia por parte de todas las partes intervinientes en el proceso.

La ponderación entre el uso de pruebas digitales y la protección de derechos constitucionales requiere la implementación de salvaguardas adecuadas, como el uso de técnicas que minimicen el impacto en la privacidad de los individuos y que aseguren el respeto a los principios de necesidad y proporcionalidad en la obtención de estas pruebas.

En este sentido, la jurisprudencia nacional y comparada ha subrayado la importancia de que las pruebas obtenidas a partir de dispositivos electrónicos o comunicaciones digitales sean obtenidas

[65] LEY N° 23.054 – También llamado Pacto de San José de Costa Rica. Sancionada: Marzo 1° de 1984. Promulgada: Marzo 19 de 1984.

mediante orden judicial y bajo condiciones estrictamente reguladas, a fin de evitar cualquier tipo de arbitrariedad.

Finalmente, el respeto a las garantías procesales, tal como lo establece el at. 18 de la constitución y la doctrina constitucional, se erige como un pilar fundamental en el uso de las pruebas digitales. Esto implica que la obtención, presentación y evaluación de dichas pruebas debe llevarse a cabo respetando los principios de legalidad, contradicción y debido proceso.

En un Estado de Derecho, la utilización de la tecnología como medio probatorio no debe sacrificar los derechos consagrados en la Constitución, sino integrarse al sistema judicial de manera que estos sean protegidos y garantizados.

El uso de pruebas digitales debe alinearse con los principios constitucionales de privacidad, legalidad y debido proceso, enmarcando siempre la actividad judicial en el respeto irrestricto a los derechos individuales y las garantías constitucionales, tal como lo ha señalado tanto la doctrina como la jurisprudencia nacional.

4.7 Derecho de defensa en juicio y protección de datos personales e intimidad

Directamente relacionado con el punto anterior, el derecho a defensa en juicio y a la protección de datos personales, son aspectos decisivos que deben ser conciliados de manera metódica.

El respeto al derecho de defensa en juicio es esencial para garantizar un proceso legal justo y equitativo.

En el ámbito del presente ensayo académico, implica que las partes involucradas deben tener acceso adecuado y oportuno a la evidencia digital presentada en su contra.

La transparencia en la obtención y presentación de la prueba digital es crucial para permitir a la defensa cuestionarla de manera efectiva, presentar contra evidencia y participar plenamente en el proceso judicial (Creswell, 2013).

Por su parte, la protección de la privacidad y los datos personales se erige como un principio clave, y su vulneración puede tener implicancias características en el derecho a la intimidad de las personas.

Es imperativo que la recolección, manejo y presentación de la evidencia digital se realicen de manera acorde con las normativas de protección de datos vigentes, asegurando que la información sensible sea tratada con el debido cuidado y respeto a los derechos fundamentales.

En este equilibrio entre el derecho de defensa y la protección de datos e intimidad, se busca evitar prácticas que puedan comprometer la equidad del proceso o poner en riesgo la privacidad de las partes.

La implementación de salvaguardias y el cumplimiento de normativas específicas contribuyen a asegurar que la introducción y evaluación de la prueba digital no infrinja derechos fundamentales y se realice en consonancia con los principios jurídicos fundamentales.

4.8 Conclusión

A modo de cierre del presente capitulo, destacamos que la aplicación de la prueba digital en el ámbito jurídico, especialmente en el caso sujeto a estudio, presenta desafíos y dificultades, los mismos requieren de especial atención, cuidado y soluciones específicas.

No debemos perder de vista que la constante evolución de la tecnología digital y la rapidez con la que surgen nuevas amenazas cibernéticas introduce complejidades adicionales en la gestión y evaluación de la evidencia digital.

A lo largo del presente capitulo, observamos que la utilización de la prueba digital puede afectar la privacidad y los datos personales, lo

que acentúa la necesidad de equilibrar la obtención de pruebas legítimas, sumado a la protección de los derechos constitucionales, especialmente en lo que respecta al derecho de defensa en juicio y la salvaguarda de datos sensibles.

La rápida obsolescencia de tecnologías y la variabilidad en los estándares de seguridad digital plantean desafíos que requieren una especial atención, es por ello que nuevamente destacamos la necesidad de implementar protocolos especializados y rigurosos para preservar su integridad y autenticidad.

La gestión efectiva de la prueba digital demanda una comprensión profunda de sus particularidades, la adaptación a la evolución tecnológica, el respeto a las garantías constitucionales y la protección de derechos fundamentales son aspectos cruciales para fortalecer la efectividad del sistema judicial en un entorno cada vez más digitalizado.

4.8 Problemas observados

Durante la presente investigación, se han identificado diversos problemas en cuanto a la gestión y evaluación de la evidencia digital;

Manipulación: La posibilidad de alterar o modificar evidencia electrónica plantea desafíos en cuanto a la autenticidad y confiabilidad de la prueba, resaltando la necesidad de técnicas forenses avanzadas y protocolos de preservación rigurosos (Palazzi, 2016).

Obsolescencia Tecnológica en palabras de Bossler:

> La falta de compatibilidad y acceso a tecnologías anticuadas puede dificultar la presentación efectiva de la evidencia digital en el proceso judicial, sumado a la falta de estándares uniformes de seguridad digital puede generar inconsistencias en la protección de la evidencia digital. (pp. 59-60)

La cadena de custodia enfrenta el desafío de la trazabilidad y seguridad de la evidencia electrónica a lo largo de su vida útil, la implementación inadecuada de la cadena de custodia puede comprometer la admisibilidad de la prueba en el juicio (Pérez, 2022).

Tomamos dimensión de que la superación efectiva de estos problemas observados demanda una combinación de enfoques técnicos, actualización constante de prácticas forenses y consideración cuidadosa de los aspectos éticos y legales.

CAPITULO QUINTO

ACTORES DEL PROCESO

5. Introducción

El presente capítulo, versa sobre los sujetos y órganos que desempeñan un papel crucial en la investigación de la estafa informática.

A lo largo de este último capítulo, se abordarán los aspectos fundamentales, de la investigación de la estafa informática en la provincia de Córdoba, como parte del mismo se explicará el manejo de la prueba en esta clase de delitos y cuál es el trabajo realizado por las Unidades Judiciales. Como así también el rol desplegado por la oficina especializada en ciberdelitos y por consiguiente la labor desplegada por la Fiscal de Instrucción de Cibercrimen de la Justicia de Córdoba

A lo largo de este capítulo se explorará la interacción entre los distintos actores judiciales, así como el papel que juegan las víctimas durante el proceso. En este contexto, se examinarán las responsabilidades de los proveedores de servicios de internet (ISP)[66], entidades bancarias y empresas privadas proveedoras de internet.

El primer segmento se centra en el análisis del rol esencial desempeñado por las Unidades Judiciales, destacando su función primordial en los primeros actos de investigación. Como así también en el papel que desempeñan los gabinetes interdisciplinarios de policía judicial y el trabajo conjunto que llevan adelante la oficina especializada en ciberdelitos y la Fiscal de Instrucción de Cibercrimen.

De la misma manera se analizará el papel que cumplen, los actores del proceso involucrados en el delito, subrayando la posición clave de cada uno de ellos.

---

66 (ISP, por sus siglas en inglés) empresas u organizaciones que ofrecen acceso a Internet y servicios relacionados a los usuarios y empresas.

Mientras que, en el segundo apartado, se explorarán las nuevas técnicas de investigación tecnológica, obtención de direcciones IP, identificación de IMEI[67], IMSI[68] MAC[69], se analizarán en detalle las herramientas y metodologías utilizadas para rastrear e individualizar a los actores involucrados en delitos informáticos.

Asimismo, se abordarán aspectos clave como el papel del agente encubierto informático, proporcionando una visión exhaustiva de las estrategias empleadas para combatir la ciberdelincuencia.

Finalmente, el capítulo concluirá con las reflexiones derivadas del análisis de cada uno de los actores, como también de las técnicas involucradas a lo largo de todo el proceso de investigación.

5.1 Sujetos y órganos intervinientes en la investigación de la estafa informática

5.1.1 Unidades Judiciales

Las Unidades Judiciales de la provincia de Córdoba constituyen entidades adscritas al ámbito del Ministerio Público Fiscal. Encargadas principalmente de llevar a cabo los primeros actos de investigación en la fase inicial del procedimiento penal, bajo la dirección de los ayudantes fiscales, quienes cuentan con el apoyo de secretarios de actuaciones. Todos ellos investidos como funcionarios del MPF, estas unidades operan

67 El IMEI (Identificador de Equipo Móvil Internacional) es un número único de identificación asignado a cada dispositivo móvil.

68 El IMSI (International Mobile Subscriber Identity) es un número único de identificación utilizado en redes móviles GSM, UMTS y LTE para identificar de manera exclusiva a un usuario de teléfono móvil

69 Media Access Control (Control de Acceso de Medios): dirección única asignada a dispositivos de red para identificarlos en una red Ethernet

de manera continua, proporcionando servicios las 24 horas del día, los 365 días del año.

La instauración de las Unidades Judiciales en la provincia de Córdoba, responde a una estrategia destinada a llevar el servicio de justicia penal a la ciudadanía, con el propósito de lograr una intervención más temprana y eficiente, garantizando celeridad en la actuación y en la preservación y tratamiento de la evidencia.

Las Unidades se encuentran distribuidas estratégicamente a largo y ancho de todo el ámbito urbano de la ciudad de Córdoba, en el gran Córdoba y en diversas localidades del interior provincial. Estas unidades conforman un modelo de descentralización operativa del servicio judicial a toda la ciudadanía.

Este enfoque descentralizado se complementa con la presencia de Unidades Judiciales Especiales, contribuyendo así a una mayor especialización y eficacia en la gestión de la justicia penal, la creación y organización de estas unidades no solo reflejan una respuesta a las demandas de la sociedad en términos de acceso a la justicia. Sino que también persiguen la optimización de la respuesta institucional en la investigación y resolución de casos, fortaleciendo la capacidad de respuesta del sistema judicial provincial.

Los empleados[70] de las Unidades Judiciales desempeñan un papel fundamental en el manejo de la evidencia digital, además de recibir denuncias y gestionar la entrega de procedimientos policiales. Estos profesionales tienen la responsabilidad de llevar a cabo la meticulosa conservación de documentos digitales, lo que implica no solo el resguardo y preservación de la evidencia electrónica, asegurando su autenticidad e integridad, sino también brindar asesoramiento integral a los damnificados.

70 Llamados comúnmente "sumariantes", en su mayoría son abogados o estudiantes de la carrera de abogacía.

La labor de los empleados abarca la aplicación de técnicas especializadas para la identificación, recopilación y presentación de pruebas digitales, garantizando su adhesión a los estándares legales y la cadena de custodia. Asimismo, los operadores jurídicos de estas Unidades desempeñan un rol activo en el asesoramiento a los damnificados, proporcionando información detallada sobre el proceso legal, sus derechos y opciones disponibles.

Este enfoque orientado al servicio contribuye a empoderar a los afectados, asegurando que estén debidamente informados y participen de manera efectiva en el desarrollo de la investigación.

5.1.2 Gabinetes interdisciplinarios

Los Gabinetes Interdisciplinarios, compuestos (entre otros) por unidades especializadas como el gabinete de tecnología forense, la división de informática forense, la unidad de equipos de computación y la unidad de equipos móviles.

Estos organismos, bajo la dirección de la dirección de análisis criminal (DAC) y tecnologías de la información, desempeñan un papel crucial en el ámbito de la investigación penal en la provincia de Córdoba. Tienen como misión obtener y analizar datos fácticos esenciales para establecer patrones criminales, delinear el mapa del delito y diseñar políticas efectivas de persecución criminal.

El gabinete de tecnología forense se especializa en la aplicación de técnicas avanzadas para el análisis de dispositivos electrónicos, mientras que la división de informática forense se centra en la identificación y preservación de pruebas digitales. La unidad de equipos de computación y la unidad de equipos móviles están dedicadas al manejo especializado de hardware, y las unidades de internet forense se enfocan en rastrear actividades en línea y analizar la evidencia digital proveniente de la web.

La tarea de estos gabinetes no solo se limita al ámbito técnico, sino que también contribuyen a la optimización de la investigación penal al proporcionar información crucial para entender el comportamiento criminal.

Este enfoque integral busca no solo esclarecer casos existentes, sino también informar el diseño de estrategias de persecución y políticas preventivas, la obtención y análisis de datos, realizados por estos gabinetes, son esenciales para la efectividad y eficiencia del sistema de justicia penal, contribuyendo al esclarecimiento de delitos y al fortalecimiento de la seguridad ciudadana.

5.1.3 Oficina Especializada en Ciberdelitos

La oficina especializada en ciberdelitos tiene como misión coordinar y desarrollar los recursos necesarios para abordar de manera eficaz la delincuencia informática, entre las funciones llevadas a cabo por este organismo. Se incluye la labor multidisciplinaria que abarca el papel de punto de contacto de la red nacional 24/7 NCMEC[71] en delitos contra la integridad sexual infantil desde 2014.

Esta función implica colaborar activamente con el centro nacional para niños desaparecidos y explotados sexualmente y los ministerios públicos fiscales en la identificación de víctimas y la resolución de casos investigados.

Adicionalmente, la oficina brinda apoyo y asesoramiento en investigaciones criminales complejas que involucran el uso de tecnologías de la información y comunicación. La cual se traduce en la elaboración de informes con sugerencias y medidas de investigación para superar los obstáculos tecnológicos en la identificación de personas

71 National Center for Missing and Exploited Children - https://www.missingkids.org/es/home

involucradas en hechos delictivos. También, esta oficina se dedica a la estadística y seguimiento de causas, facilitando la detección temprana de conexidades y brindando soporte en situaciones de demoras o dificultades en la obtención de pruebas.

En su compromiso con la innovación y desarrollo, la agencia se mantiene actualizada en técnicas y herramientas utilizadas en investigaciones de delitos complejos vinculados a nuevas tecnologías, elabora guías y protocolos estandarizados para la preservación y obtención de evidencia digital, distribuyéndolos a todas las sedes de la provincia.

La capacitación y la investigación académica son pilares fundamentales de la oficina especializada en ciberdelitos, se participa en eventos de prevención y concientización sobre el uso adecuado de las nuevas tecnologías, dirigidos a docentes, estudiantes de nivel secundario y el público en general.

Este enfoque holístico demuestra el compromiso del departamento con la formación, prevención y respuesta eficiente ante los desafíos del cibercrimen en la sociedad contemporánea.

5.1.4 Fiscalías de Instrucción

En el ámbito de la provincia de Córdoba, la función de investigación de los delitos recae en los fiscales de instrucción, quienes, con el respaldo técnico-científico y multidisciplinario de la policía judicial (anteriormente reseñados) y bajo la supervisión de un juez de garantías, desempeña un papel crucial en la etapa preparatoria de los procesos penales.

Al tomar conocimiento de una hipótesis delictiva de acción pública, los fiscales de Instrucción tienen la obligación de iniciar de oficio una investigación preparatoria. Esta fase tiene como objetivo recopilar pruebas fundamentales para respaldar una eventual acusación o, en su defecto, para determinar el sobreseimiento de la persona imputada.

En los últimos años el MPF ha priorizado la especialización, esta evolución desencadeno la creación de fueros especiales dedicados a áreas como la lucha contra el narcotráfico, penal económico y anticorrupción, así como penal juvenil. De esta manera, se han establecido fiscalías especializadas en materias específicas, como violencia familiar, delitos contra la integridad sexual, delitos complejos y delitos cometidos en entornos digitales (fiscalía de cibercrimen).

Esta especialización demuestra el compromiso del sistema judicial cordobés con la adaptación y perfeccionamiento continuo para abordar de manera efectiva los desafíos jurídicos contemporáneos.

5.1.5 Fiscalía de Instrucción de Cibercrimen de la Justicia de Córdoba

La implementación de la fiscalía de instrucción especializada en cibercrimen en provincia de Córdoba marca un hito significativo en la respuesta institucional a los delitos vinculados a la alta tecnología informática.

Su creación, respaldada por la Ley N° 10593 sancionada por la Legislatura en diciembre de 2018, refleja el reconocimiento de la creciente complejidad técnica asociada a estos delitos y la necesidad de contar con una unidad especializada para su investigación.

El reglamento N° 89/19[72] del MPF define el ámbito material de actuación de esta fiscalía, limitándolo a hechos ocurridos en la sede judicial capital, estableciendo que las denuncias relacionadas con estos delitos serán inicialmente recibidas por las unidades judiciales y fiscalías de instrucción no especializadas. En caso de que surjan hechos que

72 Fiscalía General, Política Criminal Focalizada. Fiscalía especializada en Cibercrimen. Competencia Material. 28 de febrero de 2019.-

requieran la intervención especializada en cibercrimen, serán remitidas a dicha fiscalía.

Este enfoque se alinea con la estrategia de descentralización operativa y optimización de recursos, asegurando una respuesta especializada y eficiente en la lucha contra los delitos informáticos en la jurisdicción provincial.

La fiscalía, en su ámbito de actuación, se encarga de la investigación y procesamiento de infracciones penales en las cuales la tecnología informática juega un papel determinante, ya sea como medio o fin para la comisión del delito.

Dentro de las conductas abordadas, se destacan diversos tipos de estafas informáticas, siendo las más recurrentes aquellas relacionadas con fraudes utilizando tarjetas de crédito o débito, así como fraudes informáticos mediante billeteras virtuales y plataformas como WhatsApp.

Además de lo anterior, la fiscalía asume la responsabilidad de investigar otras modalidades delictivas vinculadas a la tecnología, como extorsiones online, daños y sabotajes informáticos, abarcando de esta manera todas las formas de delitos que emergen en el contexto digital.

Un aspecto crítico de la labor de la fiscalía radica en la correcta incorporación y preservación de la prueba digital, la cual resulta determinante para su posterior valoración en el proceso penal.

La adecuada gestión de la evidencia digital es esencial para evitar nulidades y garantizar la validez de las pruebas presentadas en juicio. Esta fiscalía especializada, consciente de la volatilidad y fragilidad de la prueba digital, es la encargada de por establecer protocolos, guías prácticas, instructivos (para gabinetes y unidades judiciales). Como así también procedimientos que aseguren su adecuada preservación, contribuyendo así a la eficacia y legalidad de las investigaciones en el ámbito tecnológico.

5.1.6 La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

La Unidad Fiscal Especializada en Ciber delincuencia (UFECI) también desempeña un papel fundamental en la recolección y preservación de evidencia digital.0 dada la complejidad inherente a estos delitos cometidos en el ciber espacio, los cuales suelen involucrar el uso de tecnologías digitales y redes informáticas.

La UFECI se erige como una entidad esencial para garantizar la integridad y autenticidad de la evidencia digital recopilada en el curso de las investigaciones.

El procedimiento de recolección y preservación de evidencia digital llevado a cabo por la UFECI se rige por protocolos y estándares rigurosos, los cuales han sido establecidos para asegurar la adquisición de pruebas digitales de manera conforme a las normativas legales y jurídicas vigentes. Es esencial que dicha evidencia sea manejada de forma meticulosa, con el objetivo de evitar la alteración o manipulación de la misma, y garantizar así su admisibilidad en un proceso judicial.

La correcta gestión de la evidencia digital resulta fundamental para la efectividad de las investigaciones y para el debido proceso judicial. En tanto que dicha evidencia suele constituir un elemento central en la identificación y enjuiciamiento de los responsables de los delitos cibernéticos.

Por lo antes descripto y a los fines del presente, se considera que la UFECI se posiciona como un actor indispensable en la protección y preservación de la seguridad digital, así como en la defensa de los derechos de las víctimas de estos delitos en el ámbito legal y jurídico.

La labor desempeñada por la UFECI en la recolección y preservación de evidencia digital en el contexto de la investigación de estafas informáticas se caracteriza por su relevancia jurídica y su contribución a la efectividad del sistema de justicia en la lucha contra la ciberdelincuencia.

5.1.7 Proveedores de servicio de internet

El establecimiento de parámetros para imputar penalmente a las organizaciones, particularmente en el ámbito de empresas como los proveedores de servicios de Internet (ISP), se fundamenta en diversos criterios.

En primer lugar, se requiere que la actividad delictiva se desarrolle en el ámbito de la empresa, considerando que los ISP son organizaciones dedicadas a prestar servicios en el entorno digital.

Al mismo tiempo, es fundamental que los beneficios derivados de la actividad delictiva redunden o puedan redundar en un aumento del patrimonio de la empresa, lo que implica la posibilidad del beneficio sobre el sujeto colectivo. La imputación penal a la organización también puede surgir tanto por la conducta activa de los representantes o supervisores como por la omisión de control de directivos o supervisores.

En este contexto, se aplican teorías como la del órgano y la del defecto organizacional, donde la responsabilidad de la empresa puede derivar de la conducta de sus representantes o de la falta de controles internos que faciliten la actividad delictiva de sus miembros.

La legislación internacional, como la convención de Budapest, recomienda la imputación a la empresa en casos de delitos informáticos, aunque en el ámbito nacional se haya avanzado en la tipificación de delitos informáticos. Tal como lo evidencia la Ley 26.388, la responsabilidad penal de los ISP aún no está completamente delineada en la legislación Argentina.

En casos específicos y tal como lo señala en su obra Aboso, G.E (2022).

Se ha evaluado la responsabilidad penal de la empresa como facilitadora o partícipe necesaria en lugar de imputarle directamente las infracciones, destacando la importancia de evaluar la conducta del

> ISP en relación con la información ilícita alojada en su plataforma y su conocimiento de la misma, así como su capacidad para eliminarla. (p. 276)

Los proveedores de servicios de Internet (ISP) son responsables de garantizar la integridad y privacidad de las comunicaciones y contenidos que circulan por sus redes.

Su responsabilidad se extiende a conductas o contenidos delictivos subidos por terceros, siempre y cuando tengan conocimiento y faciliten dicha actividad a través de su plataforma tecnológica, obteniendo beneficios económicos en el proceso.

Aunque la responsabilidad penal de las empresas prestadoras de servicios de red no está claramente establecida en la legislación y jurisprudencia, se argumenta que deberían asumir esta responsabilidad, especialmente cuando no se pueda individualizar a la persona física responsable y exista un defecto organizacional.

La regulación legal de los deberes de los ISP se presenta como una alternativa necesaria para evitar que estas empresas evalúen según sus propios intereses y cálculos cuál es la mejor decisión frente a su conducta infractora.

Este enfoque se ve respaldado por expertos en investigación cualitativa, como Mason (2010), Marshall y Rossman (2016), quienes destacan la importancia de utilizar métodos rigurosos y detallados para comprender los aspectos sociales y organizacionales de manera completa.

A los fines del presente y siguiendo la misma línea de elaboración, se subraya la importancia de avanzar en criterios de imputación de responsabilidad penal a las empresas prestadoras de servicios de Internet, teniendo en cuenta no solo la culpabilidad individual. Sino también los procesos sociales u organizacionales que puedan amenazar

la convivencia social, ya sea en el ámbito físico o virtual, la responsabilidad penal por defecto organizacional se justifica desde el punto de vista de las consecuencias de la regulación y del objeto de regulación del derecho penal.

5.1.8 Operadores bancarios y empresas privadas

El análisis de la responsabilidad de las entidades bancarias en el contexto del presente trabajo revela una escasez de desarrollo doctrinario y jurisprudencial.

En contraste con la extensa literatura existente en otros ámbitos, la complejidad de este tipo de responsabilidad se acentúa debido a la naturaleza técnico-jurídica de la actividad bancaria y la evolución hacia formas electrónicas de operación.

La incorporación de nuevas tecnologías y el surgimiento de cientos de bancas electrónicas han planteado nuevos desafíos en cuanto a la responsabilidad de las entidades bancarias.

Actualmente nuestro país cuenta con numerosos precedentes jurisprudenciales, que gradualmente han llevado a categorizar los sistemas informáticos utilizados por las entidades bancarias como cosas riesgosas, lo que implica una responsabilidad objetiva por parte de las entidades, reconociendo los riesgos inherentes a estas tecnologías.

El usuario bancario, especialmente aquellos incluidos en la cartera de consumo, es considerado un consumidor con derechos y protección según la ley, la obligación de seguridad impuesta a las entidades financieras se convierte en un deber principal y autónomo. Trascendiendo la accesoriedad y exigiendo el máximo esfuerzo para prevenir daños a la persona o intereses económicos del consumidor.

El fallo Cipriano, Ricardo José y otro c/ Banco Credicoop Coop. Ltdo (2020) destaca la culpa del consumidor como un posible eximente

de responsabilidad civil. Sin embargo, esta exención debe aplicarse de manera excepcional y con un criterio restrictivo, considerando el principio de interpretación favorable al consumidor.

La responsabilidad de las entidades bancarias no se limita a la mera información proporcionada al consumidor al inicio del contrato, debe ser reiterada en cada etapa de la ejecución del contrato, particularmente en el caso de la banca electrónica, que involucra la celebración de múltiples contratos. Por cuanto la obligación de seguridad persiste y requiere una atención continua a las acciones del usuario para garantizar su protección.

En los casos de estafas informáticas y otros daños derivados de la utilización de tecnologías financieras, la responsabilidad de las entidades bancarias debe abordarse con un enfoque proactivo y de comprensión profunda de los derechos del consumidor. La evolución tecnológica debe ir de la mano con medidas de seguridad actualizadas y una constante atención a la información y protección del usuario.

En el actual contexto, donde la tecnología y las transacciones bancarias electrónicas están en constante evolución, es fundamental que las entidades bancarias asuman una responsabilidad proactiva en la prevención de estafas informáticas.

Esto implica no solo la implementación de medidas de seguridad actualizadas en sus plataformas digitales, sino también la provisión de información clara y precisa a los usuarios. Así como campañas publicitarias y programas de asesoramiento que eduquen a los clientes sobre las amenazas cibernéticas y las mejores prácticas para protegerse.

En última instancia, la prevención efectiva por parte de las entidades bancarias no solo protege a los usuarios de posibles fraudes, sino que también fortalece la confianza y la relación de estos con las instituciones financieras.

5.2 Nuevas técnicas de investigación tecnológica

5.2.1 Obtención de una IP

La obtención de una dirección IP, es esencial para la investigación de ciberdelitos, debemos reconocer que, con el avance de la tecnología, la determinación de la dirección IP pública de una conexión a Internet se ha vuelto una práctica común. Pudiendo acceder a esta información a través de servicios en línea como WhatIsMyIP[73], que facilita la identificación de la dirección IP pública asociada a una conexión específica.

En un contexto más específico, la obtención de la dirección IP local de un dispositivo dentro de una red puede lograrse utilizando comandos específicos según el sistema operativo, como el comando ipconfig[74] en Windows o Ifconfig en Macos o Linux (Denzin & Lincoln, 2011).

La legislación y regulación en el campo del derecho informático y la ciberseguridad adquieren relevancia en la obtención y uso de información relacionada con direcciones IP. El rastreo de direcciones IP puede estar sujeto a políticas de privacidad y normativas específicas, y su aplicación debe ajustarse a las leyes y regulaciones locales pertinentes.

El estudio cualitativo de ciberdelitos, como se aborda en la obra de Ditton & Short, (2019), proporciona un marco teórico y metodológico para comprender la obtención de direcciones IP en el contexto legal.

Igualmente, se puede explorar la conexión entre la obtención de direcciones IP y la investigación legal a través de encabezados de

73 WhatIsMyIP – En español cual es mi protocolo de internet

74 Comando utilizado en sistemas operativos Windows para mostrar la configuración de red de un equipo, proporciona información sobre la dirección IP, la máscara de subred, la puerta de enlace predeterminada y otros parámetros de red.

mensajes de correo electrónico. Estos encabezados contienen información sobre la ruta de un mensaje a través de diferentes servidores, lo que puede ser relevante en investigaciones legales y forenses.

El registro de actividades en sitios web, que incluye la recopilación de direcciones IP de visitantes, se convierte en una herramienta crucial para administradores de sitios web y puede tener implicaciones legales en cuanto a la privacidad y la seguridad cibernética.

5.2.2 Identificación de IMEI, IMSI y MAC

La identificación de IMEI (Identificador Internacional de Equipo Móvil), IMSI (Identificador de Suscriptor de Módulo de Identidad) y MAC (Control de Acceso de Medios) reviste una gran importancia como técnicas de investigación en el ámbito de la ciberseguridad.

Estos identificadores desempeñan roles cruciales en la identificación única de dispositivos móviles y la gestión de la conectividad de redes, siendo fundamentales para la localización de dispositivos perdidos, robados o utilizados para cometer delitos en el ciberespacio.

El IMEI, tal como lo explica en su obra Salt, Marcos G. & Polansky, Jonathan A. (2022) es un número único asignado a cada dispositivo móvil.

> Funciona como una huella digital exclusiva y es esencial para la identificación y seguimiento de dispositivos, la identificación del IMEI puede llevarse a cabo mediante la configuración del dispositivo o consultando la etiqueta en el propio dispositivo. El conocimiento del IMEI resulta crucial para rastrear la propiedad y el uso legítimo de dispositivos móviles, así como para abordar casos de robo o actividad delictiva. (p.36)

El IMSI, por otro lado y continuado con lo explicado por el maestro Salt, Marcos G. & Polansky, Jonathan A. (2022).

> Es un código único asociado a la tarjeta SIM de un dispositivo móvil y se utiliza para identificar a un usuario específico en una red de telefonía móvil, **su obtención es fundamental en investigaciones relacionadas con la actividad del usuario en la red móvil y contribuye a la identificación de los responsables en casos de ciberestafas**. (p. 52, el resaltado me pertenece)

Asimismo, la dirección MAC, utilizada para identificar dispositivos en redes locales, constituye un identificador único asignado a la interfaz de red de un dispositivo.

La identificación de IMEI, IMSI y MAC es esencial desde el punto de vista de la ciberseguridad y la evidencia digital, permitiendo el seguimiento, la identificación y la gestión de dispositivos móviles, así como la investigación de posibles actividades delictivas o violaciones de seguridad en entornos digitales

El conocimiento detallado de estos conceptos, respaldado por investigaciones como la presente, no solo fortalece las capacidades de investigación y seguridad cibernética, sino que también contribuye a la protección de individuos y organizaciones frente a amenazas digitales.

En este sentido, se destaca la importancia de continuar explorando y actualizando los conocimientos en este campo en constante evolución para seguir avanzando en la lucha contra el cibercrimen y promover un entorno digital más seguro y protegido para todos.

5.2.3 El agente encubierto informático

El agente encubierto informático desempeña una función vital en la contraprestación de delitos cibernéticos al participar en actividades en línea con el propósito de recopilar información, identificar amenazas cibernéticas y obtener pruebas en casos de delitos informáticos, incluyendo estafas en línea.

Aunque su actuación se asemeja a la de un agente encubierto en el ámbito físico, su enfoque se sitúa en el entorno digital, desde la perspectiva procesal penal, la utilización de agentes encubiertos informáticos plantea cuestiones éticas y jurídicas cruciales (González, A. 2018).

Estos agentes desempeñan un papel crucial en la detección y prevención de actividades ilícitas en línea. Como la planificación de ciberataques, el tráfico de información confidencial o la proliferación de contenido ilegal.

El agente encubierto informático se ha convertido en una herramienta esencial en la lucha contra los delitos cibernéticos, su aplicación debe gestionarse con cautela desde el punto de vista ético y legal, asegurando que la obtención de información y pruebas cumpla con los estándares requeridos.

La obra de Ditton J. y Short, E. (2019) y la orientación metodológica de Creswell, J. W. (2013) ofrecen perspectivas significativas para comprender y abordar esta compleja área de investigación y acción legal.

En el marco normativo establecido por los funcionarios de las fuerzas de seguridad o miembros del MPF autorizados, el agente encubierto digital se configura como una herramienta legal para la obtención de información en entornos digitales. Por supuesto, previo a la autorización y consentimiento, este funcionario puede ocultar o utilizar

perfiles digitales encubiertos, interactuando en línea mediante tecnologías de la información y la comunicación.

El propósito de estas acciones puede abarcar la identificación o detención de autores, partícipes o encubridores de delitos, la prevención de la consumación delictiva o la recopilación de información y pruebas necesarias para la investigación.

La función del agente encubierto aborda también aspectos relacionados con el aseguramiento de datos informáticos almacenados, el secuestro, apertura y análisis de sistemas informáticos, así como la incautación de datos y su custodia o depósito.

Estas disposiciones buscan equilibrar la eficacia en la obtención de pruebas digitales con la protección de derechos fundamentales y la legalidad en el ejercicio de las funciones de los funcionarios autorizados (González, A. 2018).

5.5 Conclusiones – Problemas observados

En el análisis detallado de los actores involucrados en la investigación de la estafa informática en la provincia de Córdoba, se ha comprobado la relevancia de todos los actores involucrados en la recepción y el manejo de la evidencia digital.

Todos los actores (Unidades Judiciales, gabinetes interdisciplinarios, Oficinas Especializadas y Fiscalías de Instrucción) desempeñan roles esenciales en los primeros actos de investigación y ante el hecho delictivo que pone en movimiento al sistema penal para el esclarecimiento de delitos cometidos en entornos digitales.

No obstante, lo anterior, se observa un desafío significativo en la carencia de un protocolo, acuerdo reglamentario o guía práctica, para receptar, manipular e incorporar al proceso.

Comprendiendo a todo tipo de prueba digital por parte de los instructores, jefes de área y ayudantes fiscales que conforman las Unidades Judiciales.

Es que esta ausencia de un protocolo ajustado al derecho, puede generar inconsistencias en la recolección, preservación y presentación de pruebas digitales, afectando la validez y autenticidad de la evidencia en el proceso penal.

Entendemos que la necesidad de establecer directrices claras y protocolos estandarizados se erige como un imperativo para superar este obstáculo y garantizar la integridad de las pruebas digitales en la investigación de la estafa informática.

En el ámbito de los sujetos vinculados al delito, desde los proveedores de servicios de internet (ISP) hasta los operadores bancarios y empresas privadas proveedoras de internet.

Se destaca la importancia de delinear de manera precisa las responsabilidades específicas de cada entidad, este esfuerzo por clarificar roles y responsabilidades contribuirá a una colaboración más efectiva y eficiente en la investigación de estos delitos.

La exploración de nuevas técnicas de investigación tecnológica, como la obtención de direcciones IP y la identificación de IMEI, IMSI y MAC, resalta la necesidad de adaptación constante ante el avance tecnológico. No obstante lo cual, esta evolución también plantea desafíos en términos de actualización y capacitación continua para los actores involucrados.

Consideramos que la respuesta jurídica a los delitos cometidos en entornos digitales, en especial el delito de estafa informática, enfrenta cruciales desafíos, desde la falta de protocolos específicos hasta la necesidad de mantenerse al día con las innovaciones tecnológicas.

El equilibrio entre la eficacia investigativa y el respeto a los derechos fundamentales requiere un enfoque integral y colaborativo que considere

los desafíos observados, proponiendo soluciones concretas para fortalecer la lucha contra la ciberdelincuencia en la era digital.

CONCLUSIÓN FINAL

La necesaria implementación de protocolos para la gestión de evidencia digital en casos de estafa informática en argentina

El presente trabajo ha abordado exhaustivamente la problemática de la estafa informática en Argentina, examinando desde el contexto histórico y marco legal hasta el análisis jurisprudencial y procesal.

Los resultados obtenidos destacan la urgencia de establecer protocolos específicos para la gestión de evidencia digital en el marco jurídico argentino, especialmente en los casos de estafa informática.

El análisis histórico y del marco normativo, tanto a nivel nacional como internacional, evidencia un escenario legal que, aunque ha mostrado ciertos avances, sigue careciendo de herramientas específicas para enfrentar la sofisticación de la ciberdelincuencia.

En particular, el delito de estafa informática, que ha proliferado y se ha perfeccionado durante la pandemia y la post-pandemia, ha desafiado los paradigmas tradicionales, exigiendo respuestas adaptadas y especializadas.

La realidad jurídica en Argentina muestra desafíos significativos, principalmente debido a la ausencia de una reforma procesal penal integral y adaptada al Convenio de Cibercriminalidad de Budapest.

La falta de normativa específica en cuanto a protocolos o guías prácticas genera vacíos que impactan negativamente en la efectividad del enjuiciamiento de delitos informáticos, al no contar con un marco adecuado para las complejidades del ámbito digital.

El examen de la jurisprudencia tanto a nivel provincial como nacional subraya la diversidad de enfoques y la necesidad de una guía más específica para la incorporación de pruebas digitales en el proceso penal.

A pesar de los esfuerzos actuales, la falta de lineamientos claros a nivel nacional para la gestión de evidencia digital sigue siendo un

obstáculo evidente en la realización de investigaciones y enjuiciamientos efectivos, especialmente considerando que el delito de estafa informática no conoce fronteras provinciales o nacionales.

La participación de actores judiciales, desde las unidades judiciales hasta las fiscalías especializadas, es fundamental en la lucha contra la estafa informática.

Sin embargo, la falta de protocolos normativos específicos, especialmente en la provincia de Córdoba, resalta la necesidad crítica de establecer directrices uniformes y detalladas para la recolección, preservación y presentación de evidencia digital en el ámbito judicial.

La ciberdelincuencia, con su naturaleza dinámica y compleja, exige un enfoque especializado y actualizado por parte del sistema legal. En este sentido, la ausencia de protocolos normativos específicos para el manejo de evidencia digital en casos de estafa informática representa una brecha crítica en la capacidad del sistema legal argentino para abordar eficientemente estos delitos.

La introducción de protocolos específicos no solo proporcionaría claridad y coherencia normativa, sino que también establecería estándares de buenas prácticas en la gestión de evidencia digital.

La uniformidad en los procedimientos, desde la recolección inicial hasta la presentación en juicio, garantizaría la integridad y autenticidad de la evidencia, fortaleciendo así la validez de los casos relacionados con estafa informática.

El desafío actual radica en identificar y subsanar las deficiencias en el manejo de evidencia digital. La legislación argentina debe evolucionar proactivamente, no solo para mantenerse al ritmo de la evolución tecnológica, sino también para anticipar las futuras demandas en el ámbito de la ciberdelincuencia.

La implementación de guías prácticas específicas no solo mejorará la eficacia de las investigaciones y procedimientos, sino que también

fortalecerá la confianza pública en la capacidad del sistema legal para abordar la ciberdelincuencia.

En virtud de la complejidad inherente al delito de estafa informática y su repercusión en el ámbito judicial de la provincia de Córdoba, resulta imperativo implementar un **Protocolo para el Manejo de Pruebas Digitales**.

Este enfoque diferenciador se erige como una postura inédita y esencial dentro del proceso penal, especialmente en nuestra jurisdicción, donde la falta de directrices claras ha generado dificultades significativas en la incorporación adecuada de evidencia digital desde el inicio del proceso.

La ausencia de un marco protocolar específico para la gestión de pruebas digitales en casos de estafas informáticas representa una preocupación sustancial para los actores judiciales involucrados.

Esta carencia no solo podría comprometer la integridad del proceso judicial, sino que también plantea una vulneración de los derechos humanos fundamentales consagrados en tratados internacionales. La garantía de los derechos procesales es esencial para asegurar la equidad y legitimidad del sistema judicial.

La omisión de un protocolo específico podría socavar los principios fundamentales de justicia, facilitando la impunidad de los responsables de delitos informáticos. Por ende, es imperativo abordar este vacío normativo de manera exhaustiva y urgente, estableciendo directrices claras y robustas que guíen la gestión de pruebas digitales en el ámbito judicial.

Este enfoque no solo fortalecerá la capacidad de los operadores judiciales para enfrentar los desafíos que presentan los casos de estafas informáticas en la era digital, sino que también consolidará el respeto por los derechos humanos en el marco de la administración de justicia.

La adopción de un protocolo robusto y especializado no solo mitigaría estas dificultades, sino que también fortalecería la efectividad y transparencia del sistema judicial, asegurando una respuesta más eficaz y justa frente a la ciberdelincuencia en la provincia.

La implementación de protocolos o guías prácticas específicas no solo satisfará esta demanda, sino que también posicionará a Córdoba en la vanguardia de la respuesta legal a la ciberdelincuencia, estableciendo así un paradigma para abordar los desafíos emergentes en la era digital.

A lo largo de la investigación, se ha corroborado la hipótesis inicial que sostenía que la adecuada incorporación de la prueba digital en los casos de estafa informática en la provincia de Córdoba es clave para fortalecer el sistema de justicia penal y aumentar la probabilidad de obtener sentencias condenatorias.

En este sentido, se propone el siguiente anexo como una herramienta fundamental para garantizar que la gestión de la evidencia digital se realice de manera eficiente y conforme a derecho, proporcionando un marco práctico que permita alcanzar sentencias justas y acordes a la complejidad de estos delitos.

ANEXO

Protocolo de incorporación de evidencia digital en casos de estafas informáticas - CÓRDOBA CAPITAL

Introducción: Bienvenidos a esta guía práctica que tiene como objetivo proporcionar información esencial para quienes hayan sido víctimas de estafas informáticas en Córdoba Capital.

Aquí encontrarán explicaciones concisas y modelos de oficio proporcionados por Cibercrimen, aplicables a cualquier estafa, independientemente de la intervención de la Fiscalía especializada.

Protocolo General de Actuación

1. **Objeto del Protocolo:**
    - Establecer pautas y procedimientos para la investigación de ciberdelitos, especialmente de la estafa informática.
2. **Generalidades:**
    - Aplicación obligatoria en todas las Unidades Judiciales de la provincia de Córdoba Capital.
3. **Principios Generales de Intervención:**
    - Accesibilidad, respeto, confidencialidad y privacidad.
4. **Principios Específicos de Intervención:**
    - Recolección, aseguramiento y transporte de pruebas sin modificar su originalidad.
    - Examen de evidencia digital por personal idóneo.
    - Documentación detallada de todas las actuaciones.

Pautas Específicas de Actuación

1. **Recepción de Denuncias:**
    - Cumplir con lo establecido en el Código Procesal Penal.
    - Comunicar de inmediato al Ministerio Público Fiscal.
    - Asegurar la prueba aportada por el denunciante.
2. **Conservación de Pruebas:**
    - Almacenar conversaciones, mensajes, imágenes relacionados con la estafa.
    - Custodiar y cuidar la prueba conforme al Protocolo.
    - Si es en formato electrónico, reenviar a una casilla oficial.
3. **Dispositivos Móviles:**

- Tomar medidas para la copia forense del dispositivo móvil para análisis.

4. **Contacto por Teléfono:**
    - Registrar el número de teléfono de quien cometió el hecho investigado.
    - Incluir el número de la víctima.
    - Adjuntar captura de pantalla.
    - Realizar verificación a través de la página web de ENACOM para identificar la empresa correspondiente y oficiar a Telecomunicaciones.

A - ESTAFA INFORMATICA CON PERJUICIO PATRIMONIAL

1. **Comprobante de Transferencia:**
    - Adjuntar el comprobante de transferencia o constancia (homebanking) que acredite la transacción.
    - Incluir detalles de la cuenta de destino: CBU/CVU o, al menos, CUIT del destinatario.
    - Solicitar este documento en el momento de la denuncia.
2. **Autorización de Levantamiento del Secreto Bancario:**
    - Consultar a la víctima si autoriza el levantamiento del "Secreto bancario".
3. **Reclamo a la Entidad Bancaria:**
    - Verificar que la víctima haya realizado el reclamo correspondiente a su entidad bancaria.
4. **Corroboración de CBU/CVU:**
    - Verificar el CBU/CVU simulando una transferencia en billetera virtual (evitar app bancaria).
5. **Oficio a la Entidad Correspondiente:**

- En caso de no contar con el comprobante, emitir un oficio a la entidad correspondiente para solicitar los movimientos registrados.

B-HACKEO DE FACEBOOK O ESTAFA A TRAVÉS DE INSTAGRAM/FACEBOOK

1. Agregar el URL del perfil hackeado o denunciado. Para obtenerlo:
    - Ingresar al perfil.
    - Presionar los tres puntitos.
    - Seleccionar "Copiar enlace del perfil". El enlace se copiará, comenzando con "http://Facebook.com/...".
2. Oficiar a Internet Forense. A continuación, adjuntar un modelo de oficio para esta situación.
3. No olvidar adjuntar capturas de pantalla del perfil afectado, objetos en venta, conversaciones, etc.
4. Si es un caso de Marketplace y la publicación persiste, incluir el URL de la publicación.
5. Cargar el oficio con firma digital y comunicar a uniintforpoljud@justiciacordoba.gob.ar.

C- ESTAFAS COMPLEJAS

Actuaciones iniciadas entre las 07:00 horas y 00:00 horas:

1. Confeccionar el oficio a COELSA utilizando el modelo proporcionado.
2. Solicitar al funcionario de turno que firme el oficio a COELSA.
3. Una vez firmado digitalmente, asignar como Co-dependencia a la UJ de Delitos Económicos.
4. Comunicar el oficio por correo electrónico a la UJ de Delitos Económicos.

5. Llamar a la UJ e informar que se ha remitido el oficio. La UJ de Delitos Económicos es responsable de comunicar a COELSA.

Actuaciones iniciadas entre las 00:00 horas y 07:00 horas:

1. Confeccionar el oficio a COELSA según el modelo proporcionado.
2. Solicitar al funcionario de turno (pro, secre, af) que firme el oficio a COELSA.
3. Comunicar el oficio digital firmado por correo electrónico a COELSA. En caso de no recibir respuesta, realizar seguimiento.

D- Descarga de Aplicaciones como TEAMVIEWER/QUICKSUPPORT:

a) Aportar e Incorporar Captura de Pantalla del Historial de Navegación del Dispositivo:

b) Capturar y adjuntar imágenes del historial de navegación del dispositivo utilizado. Se busca obtener pruebas relacionadas con la búsqueda de información en sitios web específicos, como Netflix, Mercado Libre, Visa, etc.Aportar e Incorporar Captura de Pantalla del Historial de Llamadas:

- Capturar y adjuntar imágenes del historial de llamadas telefónicas y/o historial de llamadas vía WhatsApp. Esto incluye números contactados y fechas de las llamadas.

c) Verificación de la Aplicación "TeamViewer QuickSupport":

- Si la aplicación está presente, acceder a la sección "Configuración" y visualizar archivos de registro.
- Seleccionar la opción "enviar" y remitir los archivos de registro al correo oficial de la Unidad Judicial. Incluir estos documentos en el expediente. En caso de no tener la aplicación, dejar constancia de ello.

E - Malware O Transferencia No Autorizada en Cuenta Bancaria:

- Coordinar urgentemente con personal de la Unidad de Internet Forense y el denunciante para realizar una inspección en el dispositivo utilizado durante la operación no autorizada en la cuenta bancaria.
- Advertir al denunciante que no utilice el dispositivo hasta que se realice el análisis por personal especializado de la Unidad de Internet Forense.
- Aplicar medidas urgentes relacionadas con transferencias, como bloqueos, según sea necesario.

F- Ransomware:

a) Preservación del Dispositivo:

- Realizar la preservación del dispositivo afectado antes de cualquier manipulación adicional, para facilitar el análisis forense.

b) Intervención de Informática Forense:

- En casos de manipulación del dispositivo (backup, borrado, reinstalación), dar intervención a Informática Forense para determinar:
    1. Método de intrusión.
    2. Variante de ransomware.
    3. Direcciones IP involucradas.
    4. Métodos de recuperación.

c) Investigación del Pago o "Rescate":

- Si se realizó el pago, corroborar los medios de pago. En casos de criptomonedas, rastrear hasta casas de cambio (Exchange) y realizar operaciones para convertir en moneda física.

d) Brechas de Seguridad:

- Identificar posibles brechas de seguridad, como conexiones remotas a empresas o correos electrónicos corporativos.

G. Daño Informático:

a) Especificación del Daño:

- Detallar el resultado del daño informático, incluyendo si se borraron, modificaron, eliminaron o distorsionaron archivos y el impacto resultante en la víctima.

b) Relevamiento del Dispositivo:

Realizar un relevamiento del dispositivo a través de la Unidad de Internet Forense para obtener información detallada sobre la intrusión y su consecuencia

Referencias Bibliográficas

Doctrina:

- Aboso, G. E., & Zapata, M. F. (2006). *Ciber criminalidad y derecho penal*. Ibdef.
- Aboso, G. E. (2022). *Ciberdelitos: Análisis doctrinario y jurisprudencial* (p. 276). Eldial.
- Baigún, D., & Zaffaroni, E. (2004). *Código penal y normas complementarias. Análisis doctrinal y jurisprudencial. Parte especial*. Buenos Aires: Hammurabi.
- Buompadre, J. E. (2017). *Manual de Derecho Penal. Parte especial* (3ª reimpresión, p. 476). Editorial Astrea.
- Cafferata Nores, J. (2012). *Manual de derecho procesal penal*. Córdoba: Advocatus.
- Charmaz, K. (2014). *Constructing grounded theory*. Sage Publications.
- Chilcon, S. (2019). *El Cibercrimen En El Perú y Su Incidencia En La Seguridad Nacional*. CAEN.
- Consejo de Europa. (2001). *Convención de Budapest sobre Cibercrimen*.
- Cornavaca, L. M. del M. (2021). *La introducción de prueba electrónica en el proceso civil por audiencias de Córdoba*.
- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (p. 336). Sage Publications.
- Davara Rodríguez, M. A. (1997). *Manual de derecho informático*. Pamplona: Aranzadi.
- Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. Sage Publications.
- Ditton, J., & Short, E. (2019). Studying cybercrime: A qualitative approach. En J. Wall (Ed.), *The Routledge International Handbook of Cybercrime and Society* (pp. 157-171). Routledge.
- Donna, E. A. (2001). *Derecho penal. Parte especial* (T. II-B, pp. 333-335). Rubinzal-Culzoni.
- Eguzkilore (2006, diciembre). *Delito e informática: Algunos aspectos de derecho penal material*.

- Fernández, P. (2021). Análisis de la jurisprudencia en casos de estafa informática en Córdoba. *Revista de Estudios Jurídicos*, 22(3), 180-198.
- García Ávila, R. (2019). *La prueba electrónica en el proceso penal español* (pp. 45-46 y 62).
- Gómez, A. (2018). Análisis de la prueba digital en el contexto de la estafa informática. *Revista de Derecho y Tecnología*, 9(2), 45-62.
- Gómez, L. (2017). El papel de la Fiscalía Especializada en Cibercrimen en la investigación de delitos informáticos. *Revista de Criminología y Derecho*, 25(2), 112-130.
- González, A. (2018). *Delitos informáticos: Estudio sobre las estafas en entornos digitales*. Editorial Jurídica.
- González, S. (2017). El manejo de la prueba digital en el proceso penal: Desafíos y perspectivas en casos de estafa informática. *Revista de Derecho y Tecnología*, 10(1), 78-96.
- Kaspersky, Y. (2010). *Information Security, Computer Virus, Kaspersky Lab, Computer Security*. Betascript Publishing.
- López, J. (2020). Ciberdelitos: Concepto, características y tipologías. *Revista de Derecho Informático*, 15(2), 45-64.
- Mason, J. (2010). *Qualitative researching*. Sage Publications.
- Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research*. Sage Publications.
- Martínez, R. (2019). Estándares y protocolos para la recolección, preservación y presentación de la evidencia digital en el proceso penal. *Revista de Ciencias Jurídicas*, 18(2), 125-138.
- Mendoza, G. (2022). *Contribuciones del análisis de la prueba digital en casos de estafa informática* (Tesis de maestría inédita). Universidad Nacional de Córdoba.
- Mensa González, A. (2020). *Constitución de la Provincia de Córdoba anotada* (2ª ed.).
- Montas, L. (2016). *Adquisición y admisibilidad de la evidencia digital en la justicia penal* (p. 257).
- Morales García, O. (2010). Delincuencia informática: Intrusismo, sabotaje informático y uso ilícito de tarjetas. En G. Quintero Olivares (Ed.), *La Reforma Penal de 2010: Análisis y Comentarios*. Thomson Aranzadi Reuters.

- Nuñez, S., Bazán, J., & Ruiz Moreno, I. (2021). *Código Procesal Penal de la Provincia de Córdoba, ley Nº 8123: Jurisprudencia seleccionada y sintetizada del Tribunal Superior de Justicia y de la Cámara de Acusación de Córdoba, 2000-2021* (Tomo I y II).
- Palazzi, P. (2009). *Los delitos informáticos en el código penal*. Buenos Aires: Abeledo Perrot.
- Palazzi, P. (2016). *Los delitos informáticos en el Código Penal: Análisis de la Ley 26.388*. Buenos Aires: Abeledo Perrot.
- Pecchioni, M. (2022). Delitos cometidos en entornos digitales: La estafa informática criterios generales y su relación con otras figuras delictivas. *Biblioteca Virtual de la Academia de Derecho de la Universidad Católica de Córdoba (UCC)*.
- Pérez, A. (2022). Preservación y tratamiento de la prueba digital en el proceso penal. *Revista de Derecho Procesal*, 18(3), 240-259.
- Rosende, E. (2008). *Derecho penal e informática*. Ad-Hoc.
- Rodríguez, C. (2018). Importancia de la capacitación en el manejo de la prueba digital en el ámbito penal. *Revista de Derecho y Tecnología*, 9(2), 45-62.
- Rodríguez, G., et al. (2002). Derecho penal e Internet. En J. Cremades, et al. (Coord.), *Régimen jurídico de Internet* (pp. 261-272). La Ley.
- Salt, M. G., & Polansky, J. A. (2022). *Programa de actualización y carrera de especialización en cibercrimen y evidencia digital*. @UBACIBERCRIMEN.

Sitios web:

- Google Transparency Report. (s.f.). *Estadísticas de navegación*. Google. https://transparencyreport.google.com/safe-browsing/overview
- Infoleg. (s.f.). *Infoleg*. Ministerio de Justicia y Derechos Humanos de la Nación Argentina. http://servicios.infoleg.gob.ar
- Justiniano. (s.f.). *Justiniano*. http://www.justiniano.com/
- Legislaw. (s.f.). *Legislaw*. https://www.legislaw.com.ar
- SAIJ. (s.f.). *SAIJ*. Sistema Argentino de Información Jurídica. http://www.saij.gob.ar
- Thomson Reuters. (s.f.). *Thomson Reuters*. https://www.thomsonreuters.com

Legislación:

- Anteproyecto de reforma del Código Penal de Argentina del año 2014.
- Anteproyecto de reforma del Código Penal de Argentina del año 2018.
- *Código Penal de la República Argentina*.
- *Código Procesal Penal de la Nación*.
- *Código Procesal Penal de la Provincia de Córdoba*.
- Consejo de Europa. (2001). *Convenio sobre cibercrimen*.
- Decreto 103/2007 del Poder Ejecutivo Nacional de Argentina.
- Ley de Delitos Informáticos Nº 26.388 de Argentina.

Jurisprudencia:

- Camara Apelacion Civil y Comercial de 7°, Carátula: "*Banco de la Provincia de Córdoba c/ Rivera, Vanesa Yanina",* Expte. N° 5926974, Fecha: 19/11/2021.
- Cámara Nacional Criminal y Correccional Federal, Sala Sexta. Carátula: *"G. R. y otro s/procesamiento"* - Causa N° 39779, Fecha: 3/8/2010.
- Cámara de Apelaciones en lo Penal, Penal Juvenil, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, Sala III, Carátula: "*NN s/ estafa informática*", Causa N° 21567 - Fecha: 12/09/2022.
- Tribunal Oral en lo Criminal y Correccional N° 15, Carátula: "*Lucas Alberto Dodero p.s.a. delito de defraudación mediante una técnica informática",* Causa N° 25405, Fecha:11/10/2021.
- Camara Comercial – Sala F CIPRIANO, Carátula: "*RICARDO JOSE Y OTRO c/ BANCO CREDICOOP COOP. LTDO. s/ORDINARIO Cipriano, Ricardo José y otro c/ Banco Credicoop Coop. Ltdo*". Expediente N°: 026778 – 28/11/2020.
- Juzgado en lo Civil, Comercial y Minas de San Luis*,* Carátula: *"P. L. M. A. c/ Menchini Hermanos S.A."*, Sentencia N°: 12 - 25/09/2023.