Escuela de Negocios

Universidad Siglo 21

Especialidad en Cibercrimen

Trabajo Final de Graduación

Tema: “El Derecho como política contra el cibercrimen”

Tutor: Juan Giró

Alumno: Ariel Gallo

Dni: 26898332

Salta, Agosto 2024

RESUME

Esta tesis de especialización en cibercrimen se centra en analizar la efectividad del marco legal y las políticas contra el cibercrimen en la provincia de Salta, Argentina, con énfasis en la labor de la Fiscalía Especializada en Ciberdelitos. El estudio surge en respuesta al auge de las tecnologías de la información y el consecuente aumento de nuevas formas de delincuencia digital, que plantean desafíos sin precedentes para los sistemas legales y las fuerzas del orden. La investigación evalúa la eficacia de la normativa vigente a nivel local e internacional en la prevención y persecución del cibercrimen, considerando los tipos de delitos más frecuentes en la provincia, como el grooming, las estafas virtuales y el sexting. Se examina en detalle la estructura y funcionamiento de la Fiscalía Especializada en Ciberdelitos de Salta, identificando sus fortalezas y áreas de mejora. El análisis revela que, si bien el marco legal actual ha logrado avances, aún enfrenta limitaciones significativas. La Ley 26.388 de Delitos Informáticos proporciona una base para abordar ciertos ciberdelitos, pero la rápida evolución tecnológica a menudo deja obsoletas las leyes existentes. Esto se evidencia en el aumento de casos de grooming (30% en los últimos dos años) y estafas virtuales (45% en el último año) en Salta. La Fiscalía Especializada en Ciberdelitos de Salta muestra fortalezas importantes, particularmente en su enfoque especializado y colaborativo. Sin embargo, se identifican áreas de mejora, especialmente en la necesidad de incorporar más tecnología avanzada para la investigación digital y fortalecer la cooperación interinstitucional. En conclusión, mientras la Fiscalía Especializada en Ciberdelitos de Salta ha demostrado fortalezas significativas, se requieren esfuerzos continuos para mitigar efectivamente el impacto del cibercrimen. La implementación de las estrategias propuestas, junto con una revisión y actualización constante del marco legal, será crucial para mejorar la capacidad de Salta para prevenir, investigar y perseguir los ciberdelitos de manera efectiva. Solo a través de un enfoque integral que combine legislación actualizada, recursos tecnológicos avanzados, personal altamente capacitado y colaboración interinstitucional, se podrá hacer frente a los desafíos cambiantes del cibercrimen en la provincia y proteger adecuadamente a sus ciudadanos en el entorno digital.

Palabras clave: Cibercrimen- Marco legal - Fiscalía especializada- Seguridad digital

ABSTRACT

This specialization thesis on cybercrime focuses on analyzing the effectiveness of the legal framework and policies against cybercrime in the province of Salta, Argentina, with emphasis on the work of the Specialized Cybercrime Prosecutor's Office. The study arises in response to the rise of information technologies and the consequent increase in new forms of digital crime, which pose unprecedented challenges for legal systems and law enforcement agencies. The research evaluates the effectiveness of current local and international regulations in preventing and prosecuting cybercrime, considering the most frequent types of crimes in the province, such as grooming, virtual scams, and sexting. The structure and functioning of Salta's Specialized Cybercrime Prosecutor's Office are examined in detail, identifying its strengths and areas for improvement. The analysis reveals that, while the current legal framework has made progress, it still faces significant limitations. Law 26,388 on Computer Crimes provides a basis for addressing certain cybercrimes, but rapid technological evolution often renders existing laws obsolete. This is evidenced by the increase in cases of grooming (30% in the last two years) and virtual scams (45% in the last year) in Salta. Salta's Specialized Cybercrime Prosecutor's Office shows important strengths, particularly in its specialized and collaborative approach. However, areas for improvement are identified, especially in the need to incorporate more advanced technology for digital investigation and strengthen inter-institutional cooperation. In conclusion, while Salta's Specialized Cybercrime Prosecutor's Office has demonstrated significant strengths, continuous efforts are required to effectively mitigate the impact of cybercrime. The implementation of the proposed strategies, along with constant review and updating of the legal framework, will be crucial to improve Salta's capacity to prevent, investigate, and prosecute cybercrimes effectively. Only through a comprehensive approach that combines updated legislation, advanced technological resources, highly trained personnel, and inter-institutional collaboration will it be possible to address the changing challenges of cybercrime in the province and adequately protect its citizens in the digital environment.

Keywords: Cybercrime- Legal framework- Specialized prosecutor's office- Digital security- Computer crimes

INDICE

INTRODUCCIÓN

En la era digital, el cibercrimen emergió como una amenaza significativa para la seguridad ciudadana y la estabilidad social, desafiando los marcos legales tradicionales y exigiendo una adaptación rápida de las instituciones jurídicas. Esta tesis de especialización en cibercrimen se centró en analizar la efectividad del marco legal y las políticas existentes contra el cibercrimen en la provincia de Salta, Argentina, con un énfasis particular en la labor de la Fiscalía Especializada en Ciberdelitos.

El auge de las tecnologías de la información propició nuevas formas de delincuencia que evolucionaron constantemente, planteando desafíos sin precedentes para los sistemas legales y las fuerzas del orden. En este contexto, se consideró imperativo examinar críticamente la capacidad de respuesta de las instituciones frente a delitos como el grooming, las estafas virtuales y el sexting, que mostraron un preocupante aumento en Salta en los años previos al estudio.

Esta investigación se propuso evaluar la eficacia de la normativa vigente tanto a nivel local como internacional en la prevención y persecución del cibercrimen, considerando los tipos de delitos más frecuentes en la provincia. Asimismo, se examinó en detalle la estructura y funcionamiento de la Fiscalía Especializada en Ciberdelitos de Salta, con el objetivo de identificar sus fortalezas y áreas de mejora en la lucha contra estos delitos digitales.

La relevancia de este estudio radica en su potencial para contribuir significativamente a la comprensión y mejora de las estrategias contra el cibercrimen en Salta. Al proporcionar un análisis exhaustivo de la efectividad del marco legal vigente y examinar casos concretos, se buscó identificar prácticas efectivas y áreas de oportunidad en la investigación y procesamiento de estos crímenes. Se consideró que esta información sería crucial para la formulación de políticas públicas más eficaces y la optimización de los recursos destinados a combatir el cibercrimen.

Además, la investigación se enfoca en proponer estrategias para la capacitación e incorporación de recursos humanos especializados y tecnológicos que fortalecieran la capacidad de respuesta frente al cibercrimen en la provincia. Este aspecto se consideró fundamental, teniendo en cuenta la naturaleza altamente técnica y en constante evolución de los delitos cibernéticos.

La viabilidad de esta investigación estuvo respaldada por el acceso directo a información de la Fiscalía Especializada en Ciberdelitos de Salta, la existencia de un marco legal establecido y casos de estudio disponibles para su análisis. Asimismo, la creciente

preocupación pública por la seguridad cibernética subrayó la importancia social del tema, facilitando potencialmente el acceso a recursos adicionales y fuentes de información diversas.

En última instancia, esta tesis aspiró a contribuir al fortalecimiento de la capacidad de Salta para prevenir, investigar y perseguir los ciberdelitos de manera efectiva, proponiendo mejoras concretas en el marco legal, las políticas públicas y los recursos institucionales dedicados a la lucha contra el cibercrimen. Se consideró que solo a través de un enfoque integral y adaptativo se podría hacer frente a los desafíos cambiantes del cibercrimen y proteger adecuadamente a los ciudadanos en el entorno digital cada vez más complejo de la sociedad contemporánea.

MARCO TEÓRICO

1. El Cibercrimen: Conceptualización y Alcance

1.1. Definición de cibercrimen

En primer lugar, es importante señalar que no existe una definición única para este tipo de criminalidad. Existen diversos criterios—legal, técnico, criminológico, entre otros—sobre el tema, y algunos rechazan la idea de una categoría autónoma que pueda ser considerada como delito informático. Argumentan que estos son delitos clásicos cuya naturaleza no cambia por el hecho de ser perpetrados utilizando tecnología (Saéz Capel, 2001).

La Asociación de Argentina de Derecho de Alta Tecnología, a través de la Organización para la Cooperación Económica y el Desarrollo (OCED), define el delito informático como "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos" (Paterlini, Vega, Guerriero y Velázquez, s/f, p. 1).

Otra definición propuesta describe el delito electrónico o informático como "la conducta típica, antijurídica y culpable, no ética o no autorizada, vinculada al procesador automático de datos y/o transmisiones de datos" (Ríos Patio, s/f, p. 2).

Adicionalmente, se ha caracterizado como delito informático a aquel que "sin autorización obtenga, conozca, altere o destruya información confidencial en un sistema informático" (Montano, 2008, p. 157).

Curi, et al. (2005) definen los delitos informáticos como aquellas conductas socialmente reprobables y penalmente censurables que, realizadas a través de instrumentos, sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquier bien jurídico protegido por la ley en un momento dado.

Desde una perspectiva más cercana a la teoría penal general, Anzit, et al. (2010) describen el delito informático como toda acción (u omisión) culpable llevada a cabo por un ser humano, tipificada por la ley y realizada en un entorno informático, sancionada con una pena. El elemento informático puede intervenir como medio o como objeto: actúa como medio cuando se utilizan herramientas informáticas para llevar a cabo la acción delictiva, como en el caso de usar una computadora para falsificar dinero; y como objeto cuando la acción delictiva tiene como objetivo dañar un sistema informático, por ejemplo, cuando un virus elimina información de una computadora.

Según la página web Wikipedia, un delito informático es toda acción antijurídica y culpable que se lleva a cabo a través de vías informáticas o que tiene como objetivo destruir y

dañar computadoras, medios electrónicos y redes de Internet. La criminalidad informática se refiere a la realización de actividades que, cumpliendo con los requisitos que definen un delito, se llevan a cabo utilizando un elemento informático.

Considerando estas definiciones, es necesario establecer una definición propia por lo tanto expreso que puede inferirse que los delitos informáticos son aquellos que presentan conductas típicas y antijurídicas, concretadas mediante el uso de elementos tecnológicos o nuevas tecnologías como medio para su comisión.

Es importante señalar que los delitos informáticos están intrínsecamente relacionados con la tecnología y, a lo largo del tiempo, se han perpetrado de manera silenciosa, logrando una mayor difusión con el paso de los años.

1.2. Tipos de ciberdelitos más comunes

Se clasifica, según la Organización de las Naciones Unidas (O.N.U.), en las siguientes categorías:

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Por otro lado, se identifican conductas que pueden perjudicar a los usuarios de los sistemas informáticos, tales como:

- Acceso no autorizado.
- Actos dañinos o circulación de material dañino.
- Intercepción no autorizada.

Después de presentar las definiciones pertinentes, es importante conocer cómo se denomina esta actividad delictiva cometida con la tecnología.

El Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos menciona el término "ciberdelincuencia", que se refiere al uso de tecnologías globalizadas de la información y las comunicaciones, especialmente Internet, para la comisión de actos delictivos de alcance transnacional.

Por otro lado, aquellos que se dedican a esta actividad delictiva son denominados hackers. Estas personas se enfocan en la investigación de sistemas informáticos (software), donde el intercambio de información les permite adquirir un conocimiento avanzado en materia informática. En principio, no se les considera delincuentes, ya que su objetivo, mediante la investigación, es llegar a resultados desconocidos, rozando lo ilegal, con la finalidad de crear

nuevas funciones sobre el software ya existente. También se encuentran los crackers, conocidos como "vandálicos virtuales", cuyo objetivo es romper o dañar los sistemas de seguridad de bases de datos, empresas, entidades policiales, políticas, judiciales, entre otras. Estas personas incurren directamente en actos de ilegalidad (Sain, 2010, p. 92-93).

Un informe elaborado por el F.B.I. señala que, con la aparición de Internet y el creciente acceso a esta tecnología por parte de la sociedad, surgieron delitos como el robo de identidad y las estafas, que con el tiempo evolucionaron hacia la extorsión.

Estos delitos causaron grandes perjuicios económicos y daños a los derechos personales, resultando en significativas pérdidas de dinero para las víctimas, quienes en muchos casos requirieron la intervención de profesionales como psicólogos y médicos.

El delito de robo de identidad se relaciona directamente con la extorsión, ya que la sustracción de una fotografía y datos personales puede generar consecuencias imprevistas, permitiendo al perpetrador mantenerse en el anonimato de manera indefinida.

Ante la gravedad de estos hechos y con el objetivo de regular, prevenir y combatir estas actividades delictivas para garantizar un futuro más seguro, el F.B.I. se vio en la necesidad de hacer públicos informes criminalísticos y de cooperar entre Estados para enfrentar a estos ciberdelincuentes (F.B.I., 2015).

Wikipedia clasifica los delitos informáticos en dos categorías principales:

a) Aquellos cometidos mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, donde la informática actúa como medio o instrumento para llevar a cabo el delito.

b) Aquellos cuyo objetivo es causar daños, provocar pérdidas o impedir el uso de sistemas informáticos, lo que se conoce como delitos informáticos.

En este contexto, Migliorisi (2014) divide estos ilícitos en dos grandes grupos. Por un lado, se encuentran los ciberdelitos tipificados o delitos tradicionales del Código Penal que se configuran a través de Internet. Estos son delitos históricamente tipificados en el Código Penal Argentino, cuya ejecución se realiza utilizando medios informáticos e Internet. Aunque existían antes de la creación de Internet y la informática, ahora se incorporan nuevos medios para cometerlos.

Por otro lado, Migliorisi considera que los ciberdelitos propiamente informáticos son aquellos que surgieron con la tecnología, es decir, con el nacimiento de la informática e Internet. Este grupo también incluye delitos tipificados en el Código Penal, pero cuyos efectos se han trasladado al ciberespacio, como el fraude y el daño informático.

Por su parte, el Convenio sobre Ciberdelincuencia del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001, fue el primer instrumento legal de carácter internacional sobre delincuencia informática. Este convenio estableció una clasificación de cuatro tipos de delitos:

1) Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

2) Delitos informáticos propiamente dichos.

3) Delitos relacionados con contenidos ilícitos.

4) Infracciones al derecho de autor.

2. Marco Legal del Cibercrimen

2.1. Legislación internacional sobre ciberdelitos

La proliferación de los delitos informáticos en las últimas décadas ha sido notable, especialmente en países desarrollados como Estados Unidos, Francia, España, Alemania, e Israel. En Sudamérica, Puerto Rico se destaca por haber anticipado esta problemática y sus posibles consecuencias en ausencia de legislación y regulación adecuadas. Algunos incluso han llegado a sugerir que una posible tercera guerra mundial podría librarse a través de ordenadores.

Este conflicto, denominado ciberguerra, no implicaría enfrentamientos militares tradicionales, sino la participación de personas con conocimientos informáticos dedicadas a la destrucción, daño o perjuicio de otros Estados. La gravedad de esta posible guerra se ve amplificada por el constante avance tecnológico, que deja siempre un paso atrás a quienes intentan mantener el orden o evitar un conflicto cibernético. Según M. Rogers, la NSA ya se está preparando para una guerra mundial cibernética (Muller, 2015, p.1).

Un ejemplo reciente de lo mencionado son los graves acontecimientos que han impactado al mundo, como los atentados terroristas que han afectado a ciudadanos franceses en su propio país. Estos actos han sido repudiados por numerosas personas, Estados y organizaciones.

En respuesta a los atentados en Francia, una organización no gubernamental y sin fines de lucro anunció, a través de los medios de comunicación, una venganza mediante una ciberguerra contra el Estado Islámico, quienes fueron los responsables de los ataques terroristas en ese país. En su declaración, mencionaron la intención de llevar a cabo ciberataques masivos.

Esta organización, conocida como Anonymous, se identifica por la icónica máscara blanca de Guy Fawkes que sus miembros utilizan para representarse. Anonymous está

compuesta por personas con amplios conocimientos informáticos, y es considerada la mayor red de activistas y hackers del mundo (El Día, 2015).

En este contexto, Sudamérica ha tomado nota de estos acontecimientos, y en particular, se destaca la legislación de Puerto Rico en el ámbito de los delitos informáticos. Este marco legal es considerado uno de los más avanzados, con una problemática actual controlada, respaldada por legisladores con un profundo conocimiento en la materia. Reconociendo la gravedad que puede desencadenarse con un delito informático, se subraya la importancia de evitar la impunidad y el anonimato de los ciberdelincuentes, así como la necesidad de contar con un enfoque informado y comprometido al legislar en este campo.

En Tel Aviv, Israel, uno de los principales objetivos es la lucha contra el cibercrimen, con un enfoque particular en el fraude en Internet, que se ha propagado globalmente. La O.P.C. (Organización Policial Internacional), más conocida como Interpol, celebró una reunión en Francia con representantes de cuarenta y nueve países europeos. En esta reunión, se destacó como prioridad máxima el combate contra el cibercrimen, que se está extendiendo por todo el mundo. Sin embargo, aún existen muchos países que no cuentan con medidas de seguridad informática adecuadas ni con una legislación acorde para enfrentar este tipo de delitos.

Durante la misma reunión, se presentó un informe de la Universidad Metropolitana de Londres que reveló que el 80% de los delitos en línea, es decir, aquellos cometidos con conexión a Internet, están vinculados con bandas que interactúan con miembros de diferentes partes del mundo.

En Israel, una nueva generación de bandas organizadas está surgiendo, afectando la seguridad del país. Estas bandas comienzan con el reclutamiento de miembros en otros países, especialmente aquellos sin vínculos diplomáticos con Israel. De esta manera, los líderes de estas ciberbandas, ubicados en distintos puntos del mundo, pueden tomar decisiones que luego son ejecutadas por los miembros de la organización. Internet les ha proporcionado una ventaja significativa, facilitando su migración hacia el uso de tecnología para el tráfico de datos, lo que, como se ha mencionado, les brinda una sensación de seguridad e impunidad a los ciberdelincuentes (Khoo Boon Huim, 2012).

Un ejemplo concreto de estas ciberbandas organizadas es el arresto llevado a cabo por la policía de Malasia, en el que se detuvieron a unos doscientos ciberdelincuentes de nacionalidades china y taiwanesa. Estas personas, organizadas en dos bandas bajo el mando de un único líder taiwanés, se dedicaban a cometer fraudes por internet. La banda operaba desde ubicaciones temporales en diferentes puntos de Oriente y lograba embolsarse miles de millones

de dólares mediante fraudes a tarjetas de crédito y cuentas bancarias, aprovechando sitios de fútbol y apuestas.

En Israel, se ha registrado una estadística alarmante de mil ataques diarios a la red global, lo que ha provocado pérdidas económicas millonarias. Como respuesta a esta situación, y a través de fuertes políticas de prevención y combate contra los ciberdelincuentes, la O.P.C. ha propuesto la creación de un establecimiento en Singapur con el propósito de entrenar a las fuerzas policiales del mundo en la lucha contra el delito informático (Khoo Boon Huim, 2012).

En España, la Jefatura de Estado ha promulgado una ley destinada a proteger instalaciones específicas del país contra posibles ataques, tanto físicos como cibernéticos. Por ejemplo, un ciberataque a los sistemas hidráulicos del país podría ser catastrófico, abriendo todas las represas y causando un número incalculable de muertes y devastadoras consecuencias económicas. De igual manera, un ciberataque a los sistemas de tráfico vehicular o aeronáutico podría tener resultados impactantes. Estos escenarios destacan la gravedad de los posibles ciberataques, algunos de los cuales ya han sido provocados en el pasado.

Continuando con el caso de España, el país ha promulgado la Ley 8/2011 que, en su Preámbulo, específicamente en el noveno párrafo, subraya la necesidad de crear una normativa destinada a regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo, tanto físicos como cibernéticos[1].

En China, el Ejército Popular de Liberación ha reconocido la gravedad y complejidad que implica la prevención y posterior investigación del cibercrimen. En respuesta, están preparando a sus fuerzas de seguridad para enfrentar y combatir amenazas informáticas. Este entrenamiento incluye la incorporación de tecnología de excelencia y la creación de unidades especiales en tecnología digital. China, anticipando una problemática mundial en forma de ciberguerra, se está preparando para enfrentar estas crecientes presiones internacionales debido a los ataques informáticos realizados por hackers (Infobae, 2013).

En Estados Unidos, este tipo de conflictos cibernéticos ha sido denominado "Cool War" o "Guerra Fría cibernética". La principal amenaza se origina en computadoras conectadas a Internet, y con estos dos elementos, es posible experimentar los efectos potenciales que podría causar un hacker.

La Agencia de Seguridad Mandiant emitió un informe tras una señal de alerta sobre espionaje cibernético, en el que se imputan los hechos a países como China. Varias entidades

[1] Ley 8/2011, (2011), Medidas para la Protección de las Infraestructuras Críticas. Jefatura del Estado, España.

en todo el mundo han sido víctimas de ataques por parte de ciberdelincuentes o hackers. Las investigaciones establecieron que estos ataques provenían de un edificio en Shanghái, donde se encuentra la sede de operaciones de la unidad 61398 del Ejército de Liberación Popular. El objetivo de estos ciberdelincuentes era robar todo tipo de información militar, económica y tecnológica.

En la República Argentina, no se percibe una amenaza inminente de ciberguerra o ciberataques para las fuerzas de seguridad, pero surge la pregunta de hasta qué punto el país está realmente fuera del radar de los ciberdelincuentes. En tiempos recientes, se han recibido amenazas contra la presidencia de la Nación a través de correos electrónicos dirigidos a casillas de correo gubernamentales y de fuerzas de seguridad. Estos mensajes contenían amenazas contra la vida de la presidenta, con referencias a actos violentos atribuidos al Estado Islámico.

Ante esta situación, se convocó a una reunión de todas las fuerzas federales y provinciales con el propósito de dilucidar un posible inicio de investigación, un proceso que resultó ser desconocido para todos los presentes. Frente a estos acontecimientos, surge la pregunta: ¿cuáles son las medidas preventivas o métodos investigativos a seguir? No existe una respuesta clara, ya que no se dispone de una metodología concreta para iniciar una investigación contra una o más personas con conocimientos avanzados en informática.

En el caso mencionado, los autores de las amenazas utilizaron un navegador web conocido como Red Tor, cuya principal función es garantizar el anonimato de cualquier usuario que navega por Internet. Este anonimato se logra mediante el enmascaramiento de la dirección IP original, asignando en su lugar una dirección al azar ubicada en cualquier parte del mundo. Como resultado, realizar una amenaza a través de Red Tor haría casi imposible que las fuerzas policiales de la República Argentina puedan esclarecer el hecho (División Contraterrorismo, 2015).

2.1.1. Convención de Budapest

En el ámbito de los delitos informáticos, la legislación global es escasa, dado que se trata de un tipo de crimen nuevo, difícil de investigar y con pocas herramientas preventivas. El rápido avance tecnológico de los últimos años y el aumento de actividades delictivas que utilizan la tecnología han llevado a la creación del Convenio de Budapest. Este acuerdo se ha convertido en un importante impulsor legislativo, sirviendo de modelo para que otros países adapten sus leyes.

El Convenio tiene sus raíces en Europa, una región conocida por su sólida cooperación jurídica y policial internacional en la lucha contra la delincuencia. Firmado en Budapest en 2001 y vigente desde el 1 de julio de 2004, el Convenio persigue dos objetivos principales. Primero, busca abarcar todas las áreas del Derecho Penal y Procesal relacionadas con los delitos informáticos.

En segundo lugar, aspira a ser un ejemplo legislativo para otros países, destacando la gravedad de los delitos informáticos y fomentando la cooperación internacional para prevenir y combatir este tipo de criminalidad.

El Convenio, diseñado para armonizar las legislaciones de los 47 países firmantes, está abierto a la adhesión de otros Estados.

Comienza con un Preámbulo que subraya su propósito futuro: "convencidos de la necesidad de aplicar, con carácter prioritario, una política común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular y mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional."[2]

Para lograr una uniformidad legislativa mundial en materia de delitos informáticos en el ámbito del Derecho Penal, el Convenio introduce conceptos clave en los Artículos 2 al 9.

En estos artículos, se abordan los sistemas informáticos y de datos, la falsificación y el fraude informático, el uso de tecnología computacional para crear, distribuir o procesar pornografía infantil, y el empleo de dicha tecnología para infringir la propiedad intelectual[3].

Las actividades delictivas que se centran en los sistemas informáticos y los datos incluyen el acceso no autorizado, el daño y el uso indebido de dispositivos. Además, la Convención ha abordado el Derecho Procesal, considerando los desafíos investigativos, con el fin de facilitar la ejecución de diligencias judiciales respetando las garantías constitucionales de cada Estado. En los Artículos 16 al 21, se trata la preservación y producción de pruebas digitales o evidencia virtual, así como las solicitudes de búsqueda para el secuestro de sistemas informáticos, con la debida autorización judicial para llevar a cabo las medidas protocolares[4].

Los Artículos 23 y 24 se refieren a la colaboración con la información obtenida, la preservación, interceptación y revelación de datos de tráfico y su contenido. También se aborda la extradición de ciberdelincuentes.

El objetivo procesal busca agilizar los procesos judiciales en materia de delitos informáticos. Actualmente, algunos países utilizan la legislación vigente para procedimientos

[2] Convención de Budapest, (2001). Preámbulo, 4to. Párrafo.
[3] Convención de Budapest, (2001). Preámbulo, Artículo 2-9.
[4] Convención de Budapest, (2001). Preámbulo, Artículo16-21.

de resguardo de pruebas digitales, cuando en realidad requieren un tratamiento completamente diferente. Esta práctica puede acarrear consecuencias graves, como la nulidad de una investigación.

2.1.2. Declaración del Fortalecimiento de la Seguridad Cibernética en las Américas

La tecnología se percibe como una preocupación global, y se busca, mediante la coordinación y cooperación entre Estados, prevenir y combatir los delitos informáticos. En este contexto de desarrollo tecnológico mundial, emerge la figura del terrorismo mediante el uso de la tecnología.

El objetivo es lograr tanto la prevención como el combate de estas amenazas. La Declaración del Fortalecimiento de la Seguridad Cibernética en las Américas reconoce que los actos delictivos facilitados por el avance tecnológico pueden tener un impacto futuro desestabilizador, tanto a nivel estatal como mundial.

Esta Declaración identifica los ataques cibernéticos de alto riesgo social y global, centrándose en el terrorismo como su eje principal. Su propósito es reconocer el delito de terrorismo ejecutado a través de nuevas tecnologías, buscando prevenir y combatir actos terroristas que utilizan estos medios. Además, promueve la cooperación entre Estados miembros. Es relevante citar uno de sus párrafos: "La importancia de reforzar la seguridad y la resistencia de tecnologías de infraestructura crítica de información y comunicaciones (TIC) ante las ciber amenazas, con especial énfasis en las instituciones gubernamentales críticas, así como en los sectores críticos para la seguridad nacional, incluyendo los sistemas de energía, financieros, transporte y telecomunicaciones." (Fortalecimiento de la Seguridad Cibernética en las Américas, 2012)

Se menciona la postura de la República Argentina al firmar la Declaración, con el objetivo de prevenir, impedir y mitigar las consecuencias de posibles amenazas a la infraestructura crítica, así como estar preparados para responder a tales amenazas. Se busca garantizar la seguridad de las instalaciones y de quienes las ocupan, además de fomentar que los Estados Miembros estrechen vínculos con el sector privado y la sociedad civil para

desarrollar programas de fomento de la capacidad preventiva y de protección contra las amenazas a la infraestructura crítica[5].

Esta Convención se considera relevante en relación al delito informático, ya que en sus artículos se dispone legislación en materia de Derecho Penal. Se abordan temas como "Acceso Ilícito", "Interceptación Ilícita", "Ataque a la integridad de datos", "Ataque a la integridad de sistemas", "Abuso de dispositivos", "Falsificación informática" y "Fraude informático". En cuanto a los delitos relacionados con el contenido, se incluyen "Delitos relacionados con la pornografía infantil" y "Delitos con infracciones de la propiedad intelectual y de derechos afines" (Art. 2 al Art. 10)[6].

Además, se proporciona regulación en materia de Derecho Procesal (Art. 14 de la Convención de Budapest sobre Ciberdelincuencia, 2001). Es importante destacar los artículos relacionados con la regulación de los procedimientos que tratan la prueba y el resguardo judicial, entre los que se encuentran "Condiciones y salvaguardia", "Ámbito de aplicación de las disposiciones de procedimiento", "Conservación rápida de datos informáticos almacenados" y "Conservación y revelación parcial rápida de los datos relativos al tráfico" (Art. 15 al Art. 17)[7].

2.2. Normativa en Latinoamérica sobre ciberseguridad

La intención de observar la legislación comparada, de algunos de los países de Latinoamérica, es para tener en cuenta, como dependiendo del Estado existe una legislación clara, específica, y de prioridad en delitos informáticos. También se verá cómo otros Estados, hacen mención en escasos artículos, haciendo ambigua una posible conducta delictiva cibernética. Para luego culminar con una legislación que se considera ejemplar, que sería de gran aporte para la protección jurídica de los ciudadanos argentinos.

2.2.1. Ley 21459, Ley de Delitos Informáticos, Chile.

La presente realiza un desarrollo sistemático a través de una aproximación especial a los tipos delictivos de interceptación ilícita (artículo 3), sabotaje informático (artículos 1 y 4)

[5] Disposición Nº 2/2013, Jefatura de Gabinete de Ministros, Secretaria de Gabinete y Coordinación Administrativa Subsecretaria de Tecnologías de Gestión Oficina Nacional de Tecnologías de Información.

[6] Convención de Budapest, (2001)

[7] Convención de Budapest, (2001)

y falsificación informática (artículo 5), así como también sobre las reglas de sanción y de procedimiento contempladas en la normativa.

En Chile, la Ley 21.459 aborda los delitos informáticos en unos pocos artículos:

Artículo 6º: Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas de: - Acceso ilícito Articulo 2 - Interceptación Ilícita Art 3 - Falsificación informática Art 5

Artículo 7º: Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático.

Artículo 8º: Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.0091, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos.

Adicionalmente, se incorporan circunstancias modificatorias de responsabilidad penal, en particular, como atenuante, la cooperación eficaz, y como agravantes.

Artículo 9º: Atenuante. Cooperación eficaz. Se entiende por cooperación eficaz el suministro de datos o informaciones precisas, verídicas y comprobables conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración.

Por lado, se sancionó la Ley 20.009, cuyo único fin es regular las responsabilidades cuando las conductas delictivas sean de características de robo, hurto, o extravío de tarjetas de crédito[8].

Por último, con la última actualización en materia de delitos informáticos, Chile presentó la Ley 18.168, la cual regula de una forma amplia las telecomunicaciones. En esta ley se aprecia la incorporación de las tipificaciones de la interferencia y la captación ilegítima de las señales de telecomunicaciones[9].

[8] Ley 20.009, Limita la Responsabilidad de los Usuarios De Tarjetas de Crédito por operaciones realizadas con Tarjetas Extraviadas, Hurtadas o Robadas. (2005).

[9] Ley 18168, Ley General de Telecomunicaciones, Chile. (2002).

En el país vecino de Chile se encuentra una ley escasa y ambigua, con la problemática de no incluir la conducta típica de la pornografía infantil en su legislación. También presenta muchos vacíos legales que brindan ventajas a los ciberdelincuentes y desprotección jurídica a los ciudadanos.

2.2.2. Ley N°1.160/97, Delitos Informáticos, Paraguay

En Paraguay se encuentra legislación en materia de delitos informáticos a partir del año 1997, en la cual se tipifican conductas, ampliando el espectro de conductas El Código Penal Paraguayo reconoce los siguientes delitos:

- Violación del secreto de la comunicación
- Alteración de datos
- Sabotaje de computadoras
- Operaciones fraudulentas por computadora
- Aprovechamiento clandestino de una prestación
- Perturbación de instalaciones de telecomunicaciones
- Pornografía infantil
- Intercepción, secuestro, apertura y examen de correspondencia
- Intervención de comunicaciones[10]

En Paraguay, se observa que desde hace varios años se ha implementado una legislación compleja en el ámbito de los delitos informáticos. Esta abarca una amplia gama de conductas delictivas, incluyendo la pornografía infantil y las operaciones fraudulentas, como estafas en compras, uso indebido de tarjetas de crédito y débito, y falsificaciones. Esta legislación sirve como modelo para que otros Estados adapten sus propias leyes.

Un aspecto destacable de la Ley Paraguaya es el Artículo 188°, que introduce una tipificación específica denominada "Operaciones fraudulentas por computadora". Este artículo se refiere al procesamiento indebido de datos ajenos con el fin de obtener beneficios patrimoniales. Esto puede interpretarse como acciones que incluyen la falsificación de programas o software, el uso de datos falsos o incompletos, o la utilización indebida de información[11].

Adicionalmente, la LEY N° 2861/2006 aborda de manera integral la pornografía infantil, penalizando su exhibición, reproducción y difusión. Es importante resaltar que el

[10] Ley Nº. 1.160/97, Delitos Informáticos, Paraguay, Artículos (144, 146, 173, 174, 175, 188, 189, 220). (1997).

[11] Ley Nº. 1.160/97, Delitos Informáticos, Paraguay, (1997). Artículo 188, inc. 1, 2, 3, 4.

Artículo 6º tipifica específicamente la posesión y el consumo de pornografía infantil, proporcionando así una protección exhaustiva a los menores frente a este delito[12].

2.2.3. Ley 12.737 Delitos Informáticos, Brasil.

En cuanto a Brasil, la Ley 12.737 sobre Delitos Informáticos, vigente desde 2012, establece la tipificación criminal de los delitos informáticos mediante una actualización legislativa. Uno de sus artículos más relevantes es el 154 A, que tipifica conductas como la adulteración y destrucción de datos, la instalación de virus o programas diseñados para vulnerar la seguridad de sistemas informáticos. Además, la ley también aborda la venta, distribución y disposición de dispositivos fabricados con el propósito de comprometer la seguridad de sistemas informáticos.

En sus párrafos se encuentran también tipificaciones de la violación o interceptación de las comunicaciones privadas. Como elemento novedoso, se hace mención al control de dispositivos a distancia, con un agravante de la divulgación o comercialización de esa información obtenida si se trata de una persona del alto mando del Estado.

El Artículo 266 fue modificado para permitir la aprehensión inmediata de quien realice una interrupción o perturbación de servicio telemático o informático, así como de aquel que impida su restablecimiento.

Por último, en el Artículo 298, se equipará la calificación de documento particular a las tarjetas de crédito o débito, protegiendo de esta forma los datos personales que estas contienen.

En Brasil, se encuentra la complementación legislativa con la Ley 11.829, la cual presenta una regulación del Estatuto de la Niñez y la Adolescencia. Esta ley tiene por objeto brindar protección jurídica más eficaz a los niños que son víctimas de la pornografía infantil, a través de la producción, venta y distribución. Cabe mencionar que se tipifican las conductas de adquisición y posesión del material pornográfico infantil[13].

2.2.4. Ley 1.768, Delitos Informáticos, Bolivia

[12] Ley N° 2861/06, Represión el comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces (2006).

[13] Ley 11.829, Delitos Informáticos, Brasil. (2008).

En el Código Penal de Bolivia, aparece con la reforma mediante la Ley 1.768 la cual realiza una modificación en gran parte del Código. Atendiendo a la temática que nos incumbe, el enfoque se centra en el Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el cual refiere a los Delitos Informáticos.

En esta reforma se encuentra una escasa legislación en esta temática, incorporando solo dos Artículos. El 363 bis, titulado manipulación informática, trata las intenciones de obtener de forma indebida un beneficio para sí o un tercero. También se menciona la manipulación del procesamiento o transferencias de datos (internet) que tenga como fin una actividad incorrecta, como por ejemplo una transferencia de dinero a una cuenta falsa.

En el Artículo 363 ter. se encuentran tipificadas las conductas de quien, sin autorización, se apodere, acceda, utilice, modifique, suprima o inutilice datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información. Estas acciones serán sancionadas con prestación de trabajo hasta un año o multa hasta doscientos días.

En este apartado, se observa lo escaso y lo vulnerable que puede ser el país vecino ante los delitos informáticos, dado que no tipifica con especificidad la problemática de estos delitos, quedando tanto los ciudadanos como el Estado expuestos ante los ciberdelincuentes[14].

2.2.5. Ley 27309, Delitos Informáticos. Perú

La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal. Se introducen allí los artículos 207 A, que refiere a la utilización e ingreso indebido de una base de datos o sistemas de red de computadoras, con la finalidad de alterar, ejecutar, interferir, interceptar, copiar información en tránsito (internet), o que se encuentre en la base de datos.

Por otro lado, en el Artículo 207 B, se encuentra la tipificación de daños o destrucción.

En otro orden, la Ley 28.251, mediante su actualización, incorporó los delitos contra la integridad sexual, referida a la pornografía infantil, a través de la modificación del art 183-A.

Por último, se encuentra la Ley 28.493 del año 2005, la cual tiene por objeto la regulación de la utilización de los correos electrónicos, más específicamente los de spam o correos no deseados.

[14] Ley 1.768, Delitos Informáticos, Bolivia. (1997). Artículos el 363 bis y Articulo 363 ter. -

Se observa cómo en Perú se incorpora a su cuerpo legislativo la regulación de los correos electrónicos, aspecto que hasta el momento no se ha presentado en los países ya citados[15].

Es preciso también mencionar la Ley 30963 del 17 de junio de 2019, modifica el Código Penal respecto a las sanciones del delito de explotación sexual en sus diversas modalidades, con un enfoque de protección hacia las niñas, niños, adolescentes. Incorpora nuevos delitos al Código Penal, que refieren a diversas modalidades de explotación y grados de participación en el desarrollo del delito. Asimismo, promueve recursos judiciales que se traducen en mayores garantías para las víctimas.

2.2.6. Ley Nº 53-07 2007. República Dominica, Delitos Informáticos

La Ley nº 53-07, que trata sobre crímenes y delitos de alta tecnología, fue sancionada en el año 2007 en República Dominicana. Esta ley ejemplifica y ha utilizado los términos en materia de derecho Penal y Procesal del Convenio de Budapest, pero también ha agregado en su legislación objetividad sobre las conductas de los ciberdelincuentes.

Esta Ley se creó con el fin de brindar protección a los usuarios, las bases de datos y las transferencias de datos. En sus párrafos se mencionan los fundamentos de su proyección, como el alto desarrollo tecnológico que crea nuevas modalidades delictivas no tipificadas, y cómo la falta de tipificación de estas conductas otorga un vacío legal a los infractores haciéndolos inimputables.

Además, se muestra el interés internacional que existe ante esta nueva forma de cometer delitos y cómo descansan los fundamentos de su creación en bases jurídicas internacionales[16].

Articulo 4 y destacados

El Artículo 4 de la presente Ley introduce conceptos de componentes que integran la tecnología, sumergiéndose en la materia de los delitos informáticos para proporcionar una clara interpretación de la misma al finalizar su lectura. Esto permite que una persona no idónea en materia informática pueda comprender las conductas ilícitas que se presentan.

[15] Ley 27309, Delitos Informáticos. Perú. (2005)
[16] Ley Nº 53-07. Delitos Informáticos. República Dominicana (2007).

Se mencionan definiciones de términos técnicos como computadora, código malicioso, datos, dispositivo, dispositivo de acceso, documento digital, red informática, sistema de información, sistema electrónico, sistema informático, criptografía, sistema de telecomunicaciones y sistema telemático.

Posteriormente, se abordan las acciones posibles que se pueden desarrollar mediante la informática, como clonación, acceso ilícito, afectar, delito de alta tecnología, desvío de facilidades contratadas, desvío de servicios, interceptación, pornografía infantil, señal de disparo, sin autorización y transferencia electrónica de fondos.

Finalmente, se definen los individuos involucrados: sujeto activo, sujeto pasivo y usuario.

Este artículo destaca en todo Sudamérica por ofrecer una breve descripción de cada uno de los elementos, así como de las conductas posibles realizadas mediante el uso de la tecnología.

En la descripción de las figuras legales con sus respectivas sanciones, se indica que la presente ley tiene una variedad generosa en la especificación de conductas típicas, superando a muchos otros Estados. El Capítulo I, titulado "Crímenes y Delitos contra la Confidencialidad, Integridad y Disponibilidad de datos y sistema de información", mantiene un formato de descripción de conductas típicas similares a las del resto del mundo.

El Capítulo II menciona figuras legales como atentado contra la vida de la persona, robo mediante la utilización de alta tecnología, obtención ilícita de fondos, chantaje, robo de identidad, uso de equipos para la invasión de la intimidad, difamación y atentado sexual.

En el Capítulo V se encuentran las figuras legales de los crímenes y delitos contra la nación y actos de terrorismo. Además, se establece la creación de organismos judiciales y de las fuerzas de seguridad con el fin de combatir y prevenir el delito informático, así como velar por la actualización de la ley cuando se justifique.

La Ley 53-07 ha sido creada por legisladores con conocimientos profundos en materia de delitos informáticos, resultando en una de las leyes más complejas por su redacción de conductas típicas y conceptos, pero también de fácil comprensión, destacándose notoriamente del resto del mundo[17].

También establece la creación y confección de unidades específicas de investigación de delitos informáticos. El Artículo 36 crea el Departamento de Investigaciones de Crímenes

[17] Ley Nº 53-07, Delitos Informáticos. (2007). Artículo 4, República Dominicana.

y Delitos de Alta Tecnología (DICAT), con funciones específicas de combate, prevención e investigación de delitos tecnológicos.

Los Artículos 37 y 38 detallan las funciones de apoyo a la justicia y las responsabilidades del DICAT, incluyendo la supervisión de la ejecución de la ley y la investigación de denuncias.

El Artículo 43 crea la División de Investigaciones de Delitos Informáticos (DIDI), encargada de investigar delitos relacionados con crímenes contra la humanidad.

Los Artículos 44 y 45 especifican las funciones de la DIDI, que incluyen la investigación de casos relacionados con crímenes contra la humanidad, la nación y la seguridad nacional, así como el desarrollo de análisis de amenazas informáticas y la capacitación del personal.

Esta legislación demuestra un gran interés e importancia en la formación de instituciones específicas con personal idóneo en delitos de alta tecnología, destacándose como un ejemplo potencialmente aplicable en la República Argentina.

2.3. Normativa nacional en materia de ciberseguridad

En este capítulo, se realiza un recorrido por la legislación en materia de delitos informáticos en la República Argentina, con el fin de proporcionar una noción de las leyes existentes y los tipos de conductas delictivas que tipifican.

2.3.1. Ley 26.388. Delitos Informáticos

En Argentina, la aparición de nuevas conductas delictivas que involucraban el uso de tecnología generó un vacío legal dentro del Derecho Penal, imposibilitando la aplicación de sanciones. Estas conductas delictivas también implicaban la intervención del Derecho Constitucional, ya que violaban los principios de privacidad de las personas.

Fue sancionada en el año 2008, actualizando algunos artículos en el Código Penal y tipificando conductas relacionadas a los delitos informáticos. Agregó artículos y modificó otros ya incorporados en el Código Penal argentino.

Los puntos principales que abarca, incluyen:

- Tenencia con fines de distribución por Internet u otros medios electrónicos de pornografía infantil

- Violación, apoderamiento y desvío de comunicación electrónica
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones
- Interrupción de las comunicaciones electrónicas
- Acceso ilegítimo a sistemas informáticos
- Publicación de una comunicación electrónica
- Acceso a un banco de datos personales
- Revelación de información registrada en un banco de datos personales
- Daño informático y distribución de virus
- Inserción de datos falsos en un archivo de datos personales
- Fraude informático
- Daño o sabotaje informático (Bendinelli, 2014).

Uno de los artículos más importantes y de actualidad se refiere a la protección de la integridad sexual de los menores de edad ante la exposición y uso de internet y se fundamenta en el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía[18].

Lo que busca es sancionar toda producción, distribución, importación, exportación, transmisión, posesión intencional y propaganda relacionada con la pornografía infantil, en colaboración con los Estados para su prevención.

El Artículo 128 establece penas de prisión de seis meses a cuatro años para quien produzca, financie, ofrezca, comercie, publique, facilite, divulgue o distribuya representaciones sexuales explícitas de menores de 18 años, así como para quien organice espectáculos en vivo con dichas representaciones.

El Artículo 153 penaliza con prisión de 15 días a seis meses el acceso indebido a comunicaciones electrónicas, cartas u otros documentos privados, así como su apoderamiento, supresión o desvío.

El Artículo 173 inc. 16 regula la defraudación mediante manipulación informática que altere el funcionamiento normal de sistemas informáticos o la transmisión de datos.

El Artículo 183, en su segundo párrafo, penaliza la alteración, destrucción o inutilización de datos, documentos, programas o sistemas informáticos, así como la venta, distribución o introducción de programas destinados a causar daños en sistemas informáticos.

Se señala que la aplicación de esta ha presentado desafíos procesales e investigativos debido a la falta de conocimiento, capacitación y personal idóneo en la materia. Además, se

[18] Ley 26.388 Ley de Delitos Informáticos. Argentina. (2008).

menciona la problemática legal respecto a la categorización de dispositivos como teléfonos celulares y las garantías constitucionales relacionadas con la privacidad.

Se destaca que esta no es una ley especial, sino que modifica, sustituye e incorpora figuras típicas al Código Penal vigente, con el fin de regular conductas delictivas realizadas mediante el uso de nuevas tecnologías. Las penas contempladas incluyen prisión, inhabilitación y multa.

Por otro lado, y para interpretar mejor el tema, es necesario citar el Artículo 183 del Código Penal de la Nación que tipifica el delito de daño en general, donde los posibles daños corresponden a las cosas materiales. Sin embargo, surge la pregunta sobre qué sucede cuando se daña un software, ya que este artículo no podría encuadrar tal conducta. Lo mismo ocurre si se dañan los datos que se encuentran en las bases de datos.

Finalmente, se resalta la importancia del Artículo 10, que incorpora al Artículo 183 del Código Penal de la Nación sanciones para quienes alteren, destruyan o inutilicen datos, documentos, programas o sistemas informáticos, o distribuyan programas destinados a causar daños en sistemas informáticos.

En estas circunstancias, se estaría frente a un vacío legal, considerando que en la actualidad se encuentran bases de datos en cualquier ámbito de la vida cotidiana, sean comercios, bancos, aseguradoras, etc. Para una mejor ilustración de lo mencionado sobre este Artículo, se cita el presente que reza lo siguiente: "Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado".

Ante la normativa descripta que corresponde al daño, mediante la incorporación de la Ley 26.388, se amplía la figura legal hacia los caminos de las nuevas tecnologías, donde se tiene un amplio espectro de conductas que se desarrollan con la finalidad del daño informático.

Se puede mencionar que el texto del Código Penal de la Nación sufrió un amplio cambio en sus líneas, quedando redactado de la siguiente manera: "Se impondrá prisión de un mes a dos años, al que, por cualquier medio, destruyere en todo o en parte, borrare, alterare en forma temporal o permanente, o de cualquier manera impidiere la utilización de datos o programas, cualquiera sea el soporte en que estén contenidos durante un proceso de comunicación electrónica.

La misma pena se aplicará a quien vendiere, distribuyere o de cualquier manera hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños de los descriptos en el párrafo anterior, en los programas de computación o en los datos

contenidos en cualquier tipo de sistema informático y de telecomunicaciones". Artículo 183 del Código Penal de la Nación.

En el presente se encuentra una redacción solemne que trae aparejadas confusiones donde pudiera interpretarse que el delito de daño informático se estaría cometiendo siempre que alguien introduzca algún tipo de software o programa en un sistema informático, o también en otro programa que pudiera traer aparejado consecuencias potenciales de conflictos para las personas ideales que comercializan software.

También ante estas consecuencias se puede mencionar un Dictamen de la Cámara de Senadores, ante el Artículo 153, que indica el elemento normativo incorporado al tipo: "Con respecto al actual artículo 153 del Código Penal, última parte del primer párrafo …suprimiere o desviare de su destino una correspondencia que no le esté dirigida. Es menester la presente valoración de la Cámara ya que la propuesta de origen de incorporar la expresión indebidamente en la figura legal, con el objeto de que no queden dudas para la persona deba interpretar con respecto a requerir la finalidad de la responsabilidad dolosa del autor del delito.

Esta ley actualiza el Código Penal para abordar las complejidades de la era digital, estableciendo un marco legal claro que prohíbe la analogía penal y exige la tipificación expresa de las conductas ilícitas.

Con la tecnología avanzando a un ritmo sin precedentes, la ley 26.388, se convierte en una herramienta esencial para proteger a los ciudadanos y sus derechos en el ciberespacio. Además, cierra brechas de protección jurídica para las víctimas de delitos informáticos y cumple con los compromisos internacionales, reforzando la posición de Argentina en el escenario global de la justicia penal.

También impone a individuos y entidades la obligación de implementar medidas de seguridad adecuadas para salvaguardar los bienes jurídicos y evitar la responsabilidad en la comisión de delitos informáticos. Con esta legislación, Argentina da un paso adelante en la protección contra la cibercriminalidad, aunque reconoce que el trabajo no está completo y que se requiere una actualización constante para mantenerse al día con los desarrollos tecnológicos. Es, por lo tanto, un comienzo prometedor y un llamado a la acción para una vigilancia continua y adaptación legislativa en el futuro.

Representa un hito significativo en la legislación argentina, marcando un avance en la lucha contra la ciberdelincuencia y alineándose con estándares internacionales como la Convención de Budapest. Puesto que no solo refleja el compromiso de Argentina con la cooperación internacional en la prevención y sanción de delitos informáticos, sino que también destaca la necesidad de adaptar el marco legal a las nuevas realidades tecnológicas. La jurisprudencia

argentina en materia de delitos informáticos, aunque no extensa, ofrece ejemplos claros de la interacción entre la ley y la tecnología en el ámbito judicial[19].

Los casos citados ilustran los desafíos que enfrentan los sistemas legales para mantenerse actualizados frente a la rápida evolución de la tecnología y cómo la ley en cuestión que busca abordar estas cuestiones.

La actualización constante de las leyes es crucial para garantizar que los marcos legales sean efectivos y relevantes, permitiendo así que la justicia actúe de manera adecuada en el contexto de una sociedad cada vez más digitalizada.

El 25 de marzo de 2019 se presentó ante el Senado de la Nación un proyecto de ley que busca actualizar y armonizar integralmente el Código Penal argentino. El proyecto de nuevo Código Penal tomó sin mayores cambios el tipo penal del artículo 153 bis CP en su artículo 501, el cual quedó alojado en el segmento específico dedicado a la rúbrica de los "Delitos Informáticos"

El proyecto de nuevo Código Penal acuña el daño informático como figura específica dentro del Título XXVI, referido a los delitos informáticos, en su artículo 494.

Este esfuerzo de modernización legislativa es esencial para mantener la relevancia y eficacia del marco legal en la protección de los derechos individuales y en la prevención y sanción de delitos en un mundo cada vez más digitalizado.

2.3.2. Ley 25326 de Protección de Datos Personales

Como se planteó con anterioridad esta ley, inspirada en el Convenio de Budapest, establece un marco legal para la protección de datos personales dentro de bases de datos, tanto públicas como privadas, asegurando el respeto al honor y a la intimidad individual. La misma, define claramente qué se entiende por datos personales y bases de datos, delineando los derechos del titular de los datos y las responsabilidades del administrador de la base de datos.

Además, aborda la importancia de proteger los datos personales en diversos contextos, como los contratos laborales y otras transacciones cotidianas que generan registros en bases de datos. Con la implementación de esta, se busca ofrecer una protección adecuada a la

[19] Convención de Budapest. (2001).

información personal frente a los desafíos que presenta la evolución tecnológica y los posibles vacíos legales que podrían comprometer la seguridad de los datos.

La regulación de los "datos informatizados", "archivos o bancos de datos" y "datos de usuarios" es un aspecto destacado de la misma, que intenta cerrar brechas legales y proporcionar un entorno seguro para las personas físicas y jurídicas que comparten su información personal a través de contratos. De esta manera, busca preservar principios fundamentales como la intimidad y el honor, adaptándose a las necesidades de la sociedad moderna y proporcionando un marco de seguridad jurídica en el manejo de datos personales.

La Ley 26.388, que regula la protección de datos personales en Argentina, establece un marco legal para el tratamiento de la información personal. El Artículo 2 es fundamental, ya que proporciona definiciones clave que ayudan a entender el alcance de la ley. Por ejemplo, define los "Datos Personales" como cualquier información relacionada con individuos identificados o identificables, sean personas físicas o jurídicas. Esta amplia definición es esencial para garantizar que cubra todo tipo de información que pueda afectar la privacidad de una persona.

Además, distingue entre datos personales y "Datos Sensibles", estos últimos incluyen información que podría ser utilizada de manera discriminatoria, como el origen racial o étnico, opiniones políticas, convicciones religiosas, datos genéticos, entre otros. La protección de estos datos es particularmente estricta debido a su naturaleza delicada.

El concepto de "Archivo, registro, base o banco de datos" se refiere a cualquier conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, ya sea electrónico o no. Esto incluye, pero no se limita a, bases de datos digitales y archivos físicos. También aborda el "Tratamiento de datos", definiéndolo como cualquier operación realizada con datos personales, como la recopilación, almacenamiento, modificación y transferencia de información.

Los "Datos informatizados" se refieren a aquellos datos personales procesados de manera electrónica o automatizada, lo que es cada vez más común en la era digital. Reconoce la importancia de regular estos procesos para proteger los derechos de los individuos en el contexto de las nuevas tecnologías.

La Ley 26.388 proporciona un conjunto de definiciones que son cruciales para la comprensión y aplicación de la protección de datos personales en Argentina. Estas definiciones aseguran que tanto los individuos como las entidades que manejan datos personales comprendan sus derechos y obligaciones.

En las disposiciones del artículo en cuestión, se establecen las obligaciones de los titulares de bases de datos, tanto en el sector privado como en el público. Se especifica que el titular de los datos debe incluir en su identificación un domicilio legal o representaciones en el territorio nacional. Además, se define al usuario de los datos como cualquier entidad, pública o privada, que ejecute procesos de tratamiento de datos[20].

El Artículo 3 aborda los tipos de datos que son considerados lícitos siempre que estén correctamente registrados[21].

El artículo consecutivo se enfoca en la calidad de los datos, haciendo énfasis en la exactitud de los datos registrados y el propósito de dichos registros. Se subraya la importancia de la recolección de datos a través de medios legales, evitando fraudes o acciones ilegales.

Los datos deben ser precisos, claros y actualizados cuando sea necesario. Si se detectan anomalías, el responsable de la base de datos debe eliminar, modificar o completar los datos, respetando siempre los derechos del titular de los datos, como se menciona en el Artículo 16 de la ley. El titular tiene derecho a acceder a sus datos en la base de datos y, si los datos ya no cumplen con un propósito específico, deben ser eliminados[22].

La legislación vigente contempla la protección de los individuos respecto a sus datos personales contenidos en registros, otorgándoles derechos y control sobre estos. Se establece un marco legal que permite a los individuos, previa identificación adecuada, solicitar y acceder a sus datos personales, ya sean de carácter público o privado[23].

El encargado de la gestión de dichos datos está obligado a proporcionar la información requerida en un plazo no mayor a diez días; transcurrido este período, la ley prevé mecanismos de protección de datos personales y habeas data.

Además, se aborda la cuestión de la sucesión en caso de defunción del titular de los datos, garantizando una transición clara y directa a los herederos legítimos. En cuanto a las infracciones, la ley estipula sanciones penales que incluyen penas de prisión de uno a dos meses para quienes ingresen datos falsos en un registro. Estas penas se incrementan si se suministra intencionadamente información incorrecta para su inclusión en un registro. Si el acto causa daño a una persona, la pena se incrementará hasta la mitad del mínimo y máximo establecidos.

[20] Ley 25.326 Ley de Protección de Datos Personales. (2000). Argentina, Artículo 2.
[21] Ley 25.326 Ley de Protección de Datos Personales. (2000). Argentina. Artículo 3.
[22] Ley 25.326 Ley de Protección de Datos Personales. (2000). Argentina. Artículo 16.
[23] Ley 25.326 Ley de Protección de Datos Personales. (2000). Argentina. Artículo 26

Si un funcionario público participa en un delito tipificado por esta ley mientras ejerce sus funciones, se le impondrá además una pena accesoria de inhabilitación para ocupar cargos públicos por la duración de la sentencia.

Se ha establecido en el Código Penal de la Nación que las penas oscilarán entre un mes y dos años de prisión para aquellos que, con conocimiento y sin autorización, infrinjan las medidas de seguridad de las bases de datos. Esta misma sanción se aplicará a quienes divulguen información contenida en dichas bases de datos. En el caso de que un funcionario público cometa esta infracción en el ejercicio de sus funciones, se le impondrá, además, una inhabilitación de uno a cuatro años en su cargo.

La Ley de Protección de Datos Personales establece un marco regulatorio para las conductas ilícitas y los derechos de los titulares de los datos, proporcionando una redacción precisa y detallada sobre la gestión de datos en la vida cotidiana. Asegura protección legal a la información personal suministrada, incluso cuando no se conoce la identidad del receptor de dichos datos. Por ejemplo, el caso Tanus Gustavo Daniel contra Cosa Carlos Alberto y otros, relacionado con el Habeas Data (artículo 43 de la Constitución Nacional), ilustra la aplicación de esta ley.

Además, busca asegurar la protección de los datos personales almacenados en archivos, registros, bases de datos y otros medios técnicos, ya sean de carácter público o privado, salvaguardando el derecho al honor y la privacidad de las personas.

2.3.3. Ley 26.904, Groming, o Ciberhostigamiento

La incorporación de tecnologías emergentes ha conllevado a la vulneración de derechos individuales, incrementando la exposición a riesgos cuando menores interactúan con dispositivos electrónicos y se comunican a través de internet. El término "groom" en inglés, que generalmente se refiere a la preparación o arreglo, se asocia también con conductas que buscan minar moral o psicológicamente a menores con el objetivo de manipularlos emocionalmente y, eventualmente, llevar a cabo actos sexuales.

Este comportamiento, conocido globalmente como Grooming, ha dado origen a delitos específicos, algunos de los cuales han sido recientemente tipificados en Argentina. El Ciber acoso, como se denomina en Argentina, implica acciones de un adulto dirigidas a ganar la confianza de un menor, explotando su inocencia y falta de experiencia, con el propósito de

intercambiar información que puede derivar en extorsión y, finalmente, en un acercamiento sexual.

Organizaciones como UNICEF describen el Grooming como cualquier acto intencionado de un adulto para acosar sexualmente a menores mediante internet. La O.N.G. Argentina Cibersegura, promotora de la legislación correspondiente, define el Grooming como Ciberhostigamiento, caracterizado por esfuerzos deliberados de un adulto para formar una relación con un menor, con la intención de reducir sus inhibiciones y alentar comportamientos sexuales.

Se ha observado que el fenómeno del Grooming ha suscitado preocupaciones significativas en la sociedad, especialmente en contextos donde los establecimientos que ofrecen acceso a internet, conocidos como cibercafés, no estaban sujetos a una regulación estricta. Esta falta de supervisión no proporcionaba salvaguardas contra el acceso de menores a contenido inapropiado en la web, lo que resultaba en una amenaza potencial tanto para su bienestar físico como psicológico.

Ante esta situación, la Ciudad Autónoma de Buenos Aires ha tomado medidas legislativas, implementando una ley que regula el acceso de los menores a internet en espacios comerciales, limitando el acceso a ciertos sitios web. Según el Artículo 1º de dicha ley, se exige que los establecimientos comerciales equipen todas las computadoras accesibles al público con filtros de contenido que bloqueen sitios web pornográficos[24].

Además, se otorga la autoridad a los propietarios de los establecimientos para restringir el acceso a sitios web específicos prohibidos por la ley mediante el uso de filtros[25].

Establece sanciones para los propietarios que no cumplan con estas regulaciones. Este enfoque legislativo refleja una respuesta proactiva a los desafíos presentados por la adopción de nuevas tecnologías, que han afectado los derechos de las personas y han aumentado la vulnerabilidad de los menores en su interacción con dispositivos electrónicos y comunicaciones a través de internet.

El surgimiento de ciertos delitos, aún no clasificados en la legislación argentina pero reconocidos internacionalmente como Grooming, se debe a ciertas conductas. Estas prácticas, denominadas en Argentina como Ciber acoso, involucran actos de un adulto dirigidos a establecer una relación de confianza con un menor, explotando su inocencia y falta de

[24] Ley 863, Artículo 1, Ley de Establecimiento Comerciales. (2003)
[25] Ley 863, Artículo 2-3, Ley de Establecimiento Comerciales. (2003).

experiencia. El propósito es intercambiar información que puede llevar a extorsiones y finalmente a un acercamiento sexual.

En el proceso del grooming, se identifican fases que comienzan con la creación de un vínculo de amistad, donde el menor, engañado por identidades falsas que podrían simular ser otros niños, establece contactos esporádicos que gradualmente se intensifican para ganar su confianza y ejercer control psicológico.

Tras establecer un vínculo de confianza, el ciberdelincuente, habiendo ya recabado extensa información personal del menor y su entorno familiar, procede a preparar al joven para la fase de afectación. Esta fase implica la seducción del menor a través de conversaciones de contenido sexual.

Posteriormente, se avanza a la fase de extorsión, en la cual el menor, temeroso de revelar los hechos y bajo la influencia psicológica del agresor, puede ser coaccionado para producir material pornográfico infantil o para un encuentro físico. Se analiza la conducta prohibida por la ley, que sanciona el contacto con menores mediante tecnologías electrónicas con fines de abuso sexual. Se ha introducido brevemente el concepto de grooming o acoso cibernético, destacando la preocupación social ante la falta de regulación en establecimientos con acceso a internet, como los cibercafés, donde la ausencia de control sobre el contenido pornográfico expone a los menores a riesgos.

Esto motivó la promulgación de una ley específica que regula el acceso a internet por parte de menores, limitando ciertos sitios web y estableciendo en la Ley 863 de 2003 que "Los establecimientos comerciales de la Ciudad Autónoma de Buenos Aires que ofrezcan acceso a internet deben instalar y activar filtros de contenido en todas las computadoras públicas para bloquear el acceso a sitios pornográficos" (Ley 863, 2003).

Se ha integrado una nueva disposición legal al Código Penal, designada como "Artículo 131", que estipula una pena de prisión de seis meses a cuatro años para aquellos que, utilizando medios electrónicos, telecomunicaciones o cualquier otra tecnología de transmisión de datos, establezcan contacto con menores de edad con la intención de cometer delitos contra su integridad sexual.

Esta normativa permite establecer un paralelismo con el Código Penal de Chile, específicamente con el artículo 366 quater, que regula conductas similares, pero con diferencias notables respecto a la legislación argentina[26].

[26] Código Penal de Chile, Artículo 366 quater.

El mencionado artículo chileno clasifica como delito la interacción por medios electrónicos con fines de explotación sexual de menores, imponiendo sanciones más rigurosas y detallando diversas acciones relacionadas con el grooming. Entre las conductas penalizadas se incluyen: la realización de actos de connotación sexual frente a menores de 14 años o exponerlos a material pornográfico; inducir a menores a ejecutar dichos actos; y la comisión de estos actos con menores de más de 14 años bajo amenazas.

La ley chilena también sanciona estas acciones cuando se realizan a distancia, utilizando cualquier forma de tecnología nueva, reconociendo que el contacto físico no es un requisito para la configuración del delito. Así, la ley chilena tipifica claramente estas conductas, incluso cuando no hay proximidad física entre el perpetrador y el menor. Además, la legislación se agrava en casos de suplantación de identidad o suministro de información falsa a la víctima.

Se resalta en el documento la importancia de la edad de catorce años como punto de inflexión para determinar la gravedad de los actos prohibidos, exigiendo que las amenazas se concreten cuando las víctimas superan dicha edad. Consultar la sentencia "F. L. N. s/ corrupción de menores agravada" (Expte. T.C. Nº 4924-0244) para más detalles.

2.3.4. Ley 27.078 Tecnologías de la Información y las Comunicaciones

Se hace referencia a la Ley de Tecnologías de la Información y las Comunicaciones, sancionada en 2014, que establece un marco regulatorio para los proveedores de servicios de internet. Esta legislación abarca aspectos como la explotación, licencias y precios, con el fin de fomentar el desarrollo tecnológico e informativo, protegiendo al mismo tiempo los derechos de los consumidores.

Específicamente, el Artículo 5 de la ley garantiza la inviolabilidad de las comunicaciones, incluyendo el correo electrónico y el tráfico de datos a través de redes y servicios de telecomunicaciones, permitiendo su interceptación únicamente bajo orden judicial. Además, la ley regula la actividad de los proveedores desde la emisión de licencias y requisitos administrativos hasta las sanciones por incumplimiento de la normativa, enfatizando la necesidad de ofrecer servicios de calidad y a precios justos.

El Artículo 6 introduce términos fundamentales como "Autoridad de Aplicación" y "Recursos Asociados", y define "Servicio Básico Telefónico" y "Servicio de las Tecnologías de la Información y las Comunicaciones" como aquellos que involucran el transporte y

distribución de señales o datos entre usuarios a través de redes de telecomunicaciones, sujetos a regulación específica.

La ley, por tanto, regula la interacción con el tráfico de datos y el uso de redes, ya sean inalámbricas o por cable, y aborda el concepto de "Tecnologías de la información y las comunicaciones" como un conjunto integrado de recursos, software, redes y aplicaciones esenciales para la gestión de la información[27].

En el Artículo 7 se observa cómo los conceptos específicos proporcionan un complemento a la Ley 26.388 de Delitos Informáticos, la cual presenta una ausencia de conceptos fundamentales en su estructura[28].

Se destaca el término "Acceso", que se refiere a la capacidad de ingresar a sistemas y datos; "Arquitectura Abierta", que alude a un diseño de sistemas que permite la interoperabilidad y la integración; y "Interconexión", definida como la conexión física y lógica entre redes de telecomunicaciones que posibilita la comunicación entre usuarios y el acceso a servicios de terceros.

Además, se menciona la "Red de Telecomunicaciones", que comprende los sistemas de transmisión por cables, señales inalámbricas o satelitales, y terrestres; y la "Red Local", esencial en las conexiones de interfaces, constituida por una serie de redes que incluyen tanto software como hardware, necesarios para establecer una conexión de un punto a otro. Por último, se define al "Usuario de Servicios TIC" como la entidad, ya sea individual o colectiva, que hace uso de un servicio de manera personal. Todos estos conceptos son vitales para la comprensión y el fortalecimiento del marco legal que rige las actividades delictivas informáticas[29]. Ver Fallo, “Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios".

2.3. Leyes y ordenanzas locales en Salta relacionadas con el cibercrimen

La provincia de Salta, Argentina, ha desarrollado una serie de iniciativas legales para abordar el creciente desafío del cibercrimen.

En la provincia de Salta, existen varias leyes y normativas que abordan el tema del cibercrimen. Las más relevantes:

[27] Ley 27.078 Artículo 5, Tecnologías de la Información y las Comunicaciones. (2014).
[28] Ley 27.078 Artículo 7, Tecnologías de la Información y las Comunicaciones. (2014).
[29] Ley 27.078 Artículo 7 Tecnologías de la Información y las Comunicaciones. (2014).

Ley Provincial N° 8.175/19: Esta ley creó la Fiscalía Penal especializada en Ciberdelincuencia1. Su objetivo es investigar y perseguir delitos cometidos a través de medios digitales.

Reforma del Código Procesal Penal: Se han realizado modificaciones para incluir procedimientos específicos para la investigación de delitos informáticos y la incorporación de evidencia digital2. Esto incluye la promulgación de la ley N°8386, que modifica e incorpora varios artículos al Código Procesal Penal para adaptarse a la realidad digita.

Guía de Ciberdelitos: El Poder Judicial de Salta ha publicado una guía para informar a la sociedad sobre los desafíos y riesgos del uso de herramientas digitales. Esta guía es una herramienta educativa para concienciar sobre la ciberseguridad y la prevención de delitos informáticos.

Estas leyes y guías son parte de los esfuerzos de la provincia para adaptarse a los desafíos que presenta el mundo digital y garantizar la seguridad de sus ciudadanos en el ciberespacio.

Posteriormente, en 2019, se aprobó la Ordenanza N° 15.789, que promueve la realización de campañas de concientización sobre el uso seguro de internet y redes sociales en escuelas y espacios públicos (Concejo Deliberante de la Ciudad de Salta, 2019). Esta ordenanza complementa los esfuerzos provinciales, enfocándose en la educación y prevención a nivel municipal.

Además de estas iniciativas legislativas, el Poder Judicial de Salta ha creado una Unidad Fiscal Especializada en Ciberdelitos, que trabaja en coordinación con la División de Delitos Tecnológicos de la Policía de la Provincia (Poder Judicial de Salta, s.f.). Esta unidad se encarga de investigar y perseguir delitos como fraudes en línea, robo de identidad digital y otros crímenes cometidos a través de medios informáticos.

Es importante señalar que, si bien estas iniciativas locales representan un avance significativo, la mayoría de los casos de cibercrimen en Salta aún se rigen principalmente por la legislación nacional. Esto incluye la Ley 26.388 de Delitos Informáticos (Congreso de la Nación Argentina, 2008) y la Ley 27.411 que ratifica el Convenio de Budapest sobre Ciberdelincuencia (Congreso de la Nación Argentina, 2017).

En conclusión, la provincia de Salta ha demostrado un compromiso creciente en la lucha contra el cibercrimen a través de diversas leyes y ordenanzas. Sin embargo, el rápido avance de la tecnología y la evolución constante de las amenazas cibernéticas requieren una revisión y actualización continua de estas normativas para mantener su relevancia y eficacia en la protección de los ciudadanos y sistemas informáticos de la provincia.

3. La Fiscalía Especializada en Ciberdelitos de Salta

3.1. Estructura y composición de la Fiscalía

La Fiscalía Especializada en Ciberdelitos de Salta, también conocida como Unidad Fiscal Especializada en Ciberdelitos, fue creada por el Poder Judicial de Salta para abordar de manera específica los delitos informáticos. Su estructura y composición están diseñadas para enfrentar los desafíos únicos que presentan los ciberdelitos. La Fiscalía está compuesta por un Fiscal Especializado en Ciberdelitos que lidera la unidad, Fiscales Adjuntos que asisten en las investigaciones, Peritos Informáticos expertos en análisis forense digital, Analistas de Inteligencia Digital especializados en rastreo de actividades en línea, y personal administrativo de apoyo. Esta estructura multidisciplinaria permite a la Fiscalía abordar la complejidad técnica y legal de los ciberdelitos de manera efectiva (Ministerio Público de Salta, 2020).

3.2. Funciones y competencias

Las principales funciones y competencias de la Fiscalía Especializada en Ciberdelitos de Salta incluyen la investigación de delitos informáticos, la persecución penal de los responsables, la coordinación interinstitucional con otras entidades como la División de Delitos Tecnológicos de la Policía de Salta y agencias nacionales e internacionales, el asesoramiento técnico-legal a otras fiscalías y juzgados, el desarrollo de programas de capacitación y prevención, y el análisis de tendencias en ciberdelitos. Estas funciones permiten a la Fiscalía abordar de manera integral la problemática de los delitos informáticos, desde la prevención hasta la persecución penal (Poder Judicial de Salta, 2021).

3.3. Desafíos en la investigación y persecución de ciberdelitos

La Fiscalía enfrenta varios desafíos significativos en su labor. La rápida evolución tecnológica requiere una actualización constante de conocimientos y herramientas. Los problemas de jurisdicción y territorialidad complican la aplicación de la ley, ya que los ciberdelitos a menudo trascienden fronteras geográficas. El anonimato en línea y el uso creciente de tecnologías de encriptación dificultan la identificación de los perpetradores y la obtención de evidencias. Además, la volatilidad de la evidencia digital requiere acciones rápidas y precisas para su preservación.

Otros desafíos incluyen las limitaciones de recursos, tanto en términos de equipos y software especializados como de personal altamente capacitado. El marco legal en constante evolución también presenta dificultades, ya que la legislación a menudo se queda atrás respecto a los avances tecnológicos, creando vacíos legales que deben ser abordados (Asociación de Fiscales de Argentina, 2022).

Para enfrentar estos desafíos, la Fiscalía Especializada en Ciberdelitos de Salta trabaja en la mejora continua de sus capacidades técnicas, la formación constante de su personal y la colaboración estrecha con otras instituciones nacionales e internacionales dedicadas a combatir el cibercrimen. Este enfoque integral y adaptativo es fundamental para mantenerse al día con las cambiantes tácticas de los ciberdelincuentes y para proporcionar una respuesta efectiva a los delitos informáticos en la provincia de Salta.

4. Ciberdelitos en Salta

4.1. Grooming: características y consecuencias

El grooming es uno de los ciberdelitos más preocupantes en Salta, especialmente por su impacto en menores de edad. Se caracteriza por el acoso sexual a niños y adolescentes a través de medios digitales, donde un adulto se gana la confianza del menor con fines de abuso sexual.

En Salta, se ha observado un uso predominante de redes sociales y aplicaciones de mensajería para este fin, con acosadores que crean perfiles falsos y emplean manipulación psicológica gradual. Las consecuencias para las víctimas son severas, incluyendo trauma psicológico, problemas de autoestima y, en algunos casos, abuso sexual físico. Según datos de la Fiscalía Especializada en Ciberdelitos de Salta, se ha registrado un aumento del 30% en las denuncias por grooming en los últimos dos años, lo que subraya la gravedad del problema (Fiscalía Especializada en Ciberdelitos de Salta, 2023).

4.2. Estafas virtuales: modalidades y prevención

Las estafas virtuales representan una proporción significativa de los ciberdelitos en Salta, afectando a personas de todas las edades y niveles socioeconómicos.

Las modalidades más comunes incluyen el phishing, las estafas románticas, los fraudes de compra-venta en línea y los esquemas piramidales virtuales. Para combatir estas amenazas, se recomiendan medidas de prevención como verificar la autenticidad de los sitios web y

correos electrónicos, no compartir información personal o financiera sin verificación, usar contraseñas fuertes y mantener actualizado el software de seguridad. La Policía Cibernética de Salta ha reportado un incremento alarmante del 45% en denuncias por estafas virtuales durante el último año, con pérdidas económicas estimadas en varios millones de pesos (Policía de Salta, División de Delitos Tecnológicos, 2023).

4.3. Sexting: riesgos y aspectos legales

El sexting, práctica de enviar mensajes, fotos o videos de contenido sexual a través de dispositivos móviles, ha ganado prevalencia entre los jóvenes salteños, presentando riesgos significativos y desafíos legales.

El sexting, por su parte, ha ganado prevalencia entre los jóvenes salteños, presentando riesgos significativos y desafíos legales. En el ámbito legal, aunque no existe una ley específica sobre sexting en Salta, se enmarca en delitos contra la intimidad. La difusión no consentida de imágenes íntimas es punible bajo el artículo 155 del Código Penal Argentino, y cuando involucra a menores, puede considerarse producción y distribución de pornografía infantil.

Estos casos de estudio revelan la complejidad y diversidad de los ciberdelitos en Salta. Las autoridades locales, incluyendo la Fiscalía Especializada en Ciberdelitos, continúan trabajando en estrategias de prevención, investigación y persecución de estos delitos, adaptándose a las nuevas modalidades que surgen con la evolución tecnológica.

En diciembre de 2019, el Ejecutivo provincial sancionó la ley 8175/19 por la que creó la Fiscalía especializada en Ciberdelincuencia en Salta. Con la norma, la provincia vino a alinearse con la política criminal fijada a nivel internacional de perseguir aquellas conductas delictivas cometidas a través de la red, sumándose de este modo a las organizaciones más modernas de nuestro país y del mundo entero.

En Salta, como en el resto de Argentina, el sexting puede tener consecuencias legales si se difunden imágenes íntimas sin el consentimiento de la persona involucrada. Esto puede ser considerado un delito de violación de la privacidad y puede llevar a sanciones penales.

Además, si alguien utiliza imágenes íntimas para extorsionar a otra persona, esto se conoce como sextorsión y es un delito grave. Las víctimas pueden denunciar estos casos a través de varias vías, como la línea gratuita 137, presentándose en una fiscalía, o contactando a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

METODOLOGIA

La investigación se llevó a cabo utilizando una metodología cualitativa. Al respecto, "la investigación cualitativa proporciona profundidad a los datos, dispersión, riqueza interpretativa, contextualización del ambiente o entorno, detalles y experiencias únicas" (Hernández Sampieri, Baptista y Fernández, 2008, p. 21).

Se adoptó este tipo de metodología porque, como plantean Taylor y Bogdan (1994), permite al investigador observar el escenario y a las personas desde una perspectiva global.

La investigación partió de una metodología cualitativa de tipo descriptiva, buscando describir lo investigado a partir de una aproximación a los fenómenos que ocurren en determinadas situaciones o contextos (Hernández Sampieri, 2009).

El muestreo fue de carácter intencional, priorizando la selección de casos típicos, preferentemente divergentes, que reflejaran un amplio rango de situaciones. Esta diversidad permitió, en el proceso inductivo, determinar similitudes (rasgos generalizables) y diferencias (rasgos atribuibles al carácter idiosincrático, factores contextuales, etc.). La estrategia de selección cualitativa se basó en la diversidad y heterogeneidad de los casos, que fueron valiosos en la medida en que poseyeron información relevante para los fines del estudio (Yuni, 2002).

La muestra seleccionada para las entrevistas incluyó a la Fiscal Especializada en Ciberdelitos, Dra. Sofía Cornejo, quien lidera la fiscalía. La estructura de esta fiscalía está compuesta por la Fiscal, dos auxiliares fiscales que colaboran directamente en la investigación y gestión de los casos, y un equipo de ocho sumariantes encargados de realizar las investigaciones preliminares y recabar pruebas necesarias en los casos de ciberdelitos.

Para la recolección de datos, se utilizaron entrevistas escritas en profundidad. A través de esta técnica, se buscó que los propios sujetos participantes pudieran expresar sus puntos de vista e ideas sobre los procesos, momentos, situaciones o factores relacionados con la problemática planteada en la investigación.

RESULTADOS / DIAGNOSTICO

El cibercrimen representa un desafío creciente para las instituciones de justicia en todo el mundo, y la provincia de Salta no es una excepción. En este contexto, se ha llevado a cabo un análisis exhaustivo de la efectividad del marco legal y las políticas contra el cibercrimen en Salta, con un enfoque particular en la labor de la Fiscalía Especializada en Ciberdelitos.

Este estudio se basa en entrevistas en profundidad que implican encuentros cara a cara entre el investigador y los informantes, encuentros que están dirigidos hacia la comprensión de las perspectivas que tienen los informantes, en relación a sus experiencias o situaciones. Las mismas fueron realizadas a figuras clave dentro de la Fiscalía, incluyendo la Fiscal Especializada, un Fiscal Auxiliar y un Sumariante. Sus perspectivas y experiencias proporcionan una visión integral de los desafíos actuales, las fortalezas existentes y las áreas de mejora en la lucha contra el cibercrimen en la provincia.

Los resultados que se presentan a continuación ofrecen un diagnóstico detallado de la situación actual, abordando la eficacia de la normativa vigente, la estructura y funcionamiento de la Fiscalía, y las necesidades de recursos y capacitación. Este análisis servirá como base para proponer estrategias que fortalezcan la capacidad de respuesta frente al cibercrimen en Salta.

Con esta entrevista se pretendía conocer el punto de vista del profesional en cuanto al tema en cuestión. A este efecto era necesario proporcionar y facilitar las pistas y los elementos de trabajo para conseguir los datos que se querían obtener. Por lo tanto, era preciso considerar y tener en cuenta múltiples aspectos para llevar a cabo esta entrevista, se le dio a conocer en primer lugar los objetivos vertidos en este trabajo de investigación, luego se procedió a informar demás detalles de la misma.

Por lo tanto se procede al análisis e interpretación de las mismas tomando como eje las preguntas de las entrevistas.

1. Evaluación de la eficacia normativa

El marco legal actual en Salta para combatir el cibercrimen muestra avances, pero aún enfrenta desafíos significativos. La Dra. Sofía Cornejo, Fiscal Especializada en Ciberdelitos, señala: "Aunque contamos con normativas locales y nos alineamos con algunas internacionales, la rápida evolución de las tecnologías y las tácticas de los ciberdelincuentes nos exige una actualización constante." Además, agrega que "Comparada con la legislación

internacional, nuestra normativa presenta lagunas que dificultan la persecución efectiva de estos delitos, especialmente en casos que trascienden fronteras."

El Fiscal Auxiliar refuerza esta perspectiva: "En la práctica, las leyes vigentes nos permiten actuar en varios casos, pero hay áreas donde la legislación es insuficiente, especialmente en lo que respecta a la rapidez de la respuesta y la cooperación internacional."

Los tipos de cibercrimen más frecuentes en Salta incluyen "el grooming, las estafas virtuales y el sexting", según la Dra. Cornejo. La Fiscalía aborda estos delitos con un enfoque preventivo y reactivo, pero enfrenta desafíos en su persecución, como "la rápida evolución tecnológica, la dificultad para rastrear a los delincuentes que actúan desde otras jurisdicciones y la falta de recursos suficientes para investigar a fondo cada caso."

2. Estructura y funcionamiento de la Fiscalía Especializada en Ciberdelitos:

La Fiscalía cuenta con una estructura especializada, como describe la Dra. Cornejo: "La Fiscalía está compuesta por un equipo especializado que incluye dos auxiliares fiscales y ocho sumariantes, además de mí como fiscal titular." Esta estructura permite una dedicación exclusiva al cibercrimen, lo que se considera una fortaleza.

El Fiscal Auxiliar destaca la organización interna: "La Fiscalía está organizada en equipos que se especializan en diferentes áreas del cibercrimen. [...] Trabajamos de manera muy colaborativa, lo que nos permite abordar los casos de manera integral y eficiente."

Entre las fortalezas identificadas se encuentran la especialización, la capacitación continua y la colaboración interna. Sin embargo, también se identifican áreas de mejora, principalmente en recursos tecnológicos y humanos. El Fiscal Auxiliar menciona: "Una de las áreas clave que necesitamos fortalecer es la tecnología que utilizamos. [...] También sería beneficioso ampliar nuestro equipo con más especialistas en ciberseguridad y análisis forense digital."

3. Estrategias para capacitación e incorporación de recursos:

La capacitación continua se identifica como crucial en todos los niveles de la Fiscalía. La Dra. Cornejo enfatiza: "La capacitación continua es fundamental. El cibercrimen es un campo dinámico y en constante cambio, por lo que el personal debe estar siempre actualizado sobre las últimas tendencias, herramientas y métodos de investigación."

En cuanto a la incorporación de recursos, se identifica la necesidad de más personal especializado y tecnología avanzada. El Fiscal Auxiliar sugiere: "La incorporación de más recursos humanos con formación especializada, como analistas de ciberseguridad y expertos en forense digital, sería muy beneficiosa. Además, la adquisición de tecnologías avanzadas, como software para el análisis de big data y herramientas de rastreo de actividades en la dark web, mejoraría considerablemente nuestra capacidad de respuesta."

El Sumariante de la Fiscalía respalda esta necesidad: "Sería beneficioso contar con más recursos humanos especializados, especialmente en áreas como la criptografía y el análisis de redes complejas. Además, la incorporación de tecnologías más avanzadas para el análisis forense digital y la detección de actividades sospechosas en tiempo real mejoraría significativamente nuestra capacidad de respuesta."

En conclusión, mientras la Fiscalía Especializada en Ciberdelitos de Salta muestra fortalezas en su estructura y especialización, enfrenta desafíos significativos en términos de recursos tecnológicos, capacitación continua y adaptación a un panorama de cibercrimen en constante evolución. La actualización del marco legal, la mejora en la cooperación internacional y la inversión en recursos humanos y tecnológicos se presentan como áreas clave para fortalecer la lucha contra el cibercrimen en la provincia.

PLAN DE IMPLEMENTACIÓN

El siguiente plan de implementación se ha desarrollado como respuesta a los desafíos que el cibercrimen presenta para la sociedad salteña. Este plan es el resultado de un análisis exhaustivo de la situación actual, basado en entrevistas con miembros clave de la Fiscalía Especializada en Ciberdelitos y un estudio detallado de las capacidades y necesidades existentes.

Ante la rápida evolución del cibercrimen, se requiere una respuesta igualmente ágil y efectiva de las instituciones. El plan que se presenta a continuación se enfoca en seis áreas estratégicas:

1. Actualización del Marco Legal
2. Fortalecimiento de Recursos Humanos
3. Mejora de Recursos Tecnológicos
4. Mejora de la Cooperación Interinstitucional
5. Programa de Prevención y Concientización
6. Monitoreo y Evaluación

Cada una de estas áreas ha sido cuidadosamente considerada para abordar las brechas identificadas en el sistema actual y para fortalecer la capacidad de prevenir, detectar y perseguir el cibercrimen.

Este plan no solo busca mejorar la eficacia de las instituciones, sino también educar y proteger a la comunidad. Con su implementación, se aspira a crear un entorno digital más seguro para todos los salteños y a posicionar a la provincia como un referente en la lucha contra el cibercrimen.

A continuación, se detallarán cada componente del plan, sus objetivos específicos y las acciones concretas que se proponen para su implementación. Se invita a todos los sectores involucrados a aportar comentarios y sugerencias, ya que el éxito de este plan dependerá del compromiso y la colaboración colectiva.

La presentación detallada del plan comienza a continuación.

1. Actualización del Marco Legal

1.1 Crear un comité de revisión legislativa:

- Integrado por expertos en derecho penal, ciberseguridad y representantes de la Fiscalía Especializada en Ciberdelitos.

- Objetivo: Identificar lagunas en la legislación actual y proponer actualizaciones.

1.2 Desarrollar propuestas legislativas:

- Enfocadas en agilizar los procesos de investigación y persecución de ciberdelitos.

- Incluir disposiciones para mejorar la cooperación internacional.

1.3 Promover la armonización con estándares internacionales:

- Adaptar la legislación local a las mejores prácticas internacionales en materia de cibercrimen.

2. Fortalecimiento de Recursos Humanos

2.1 Programa de capacitación continua:

- Desarrollar un currículum especializado en cibercrimen para todo el personal de la Fiscalía.

- Implementar talleres trimestrales sobre nuevas tecnologías y técnicas de investigación.

2.2 Contratación de especialistas:

- Incorporar analistas de ciberseguridad y expertos en forense digital.

- Crear puestos para especialistas en criptografía y análisis de redes complejas.

2.3 Programa de intercambio y colaboración:

- Establecer acuerdos con otras jurisdicciones para intercambio de conocimientos y experiencias.

- Fomentar la participación en conferencias y seminarios internacionales sobre cibercrimen.

3. Mejora de Recursos Tecnológicos

3.1 Evaluación de necesidades tecnológicas:

- Realizar un inventario detallado de las herramientas actuales y las necesidades futuras.

- Priorizar la adquisición de tecnologías clave.

3.2 Adquisición de software especializado:

- Invertir en herramientas avanzadas para análisis forense digital.
- Adquirir software de inteligencia artificial para análisis de big data y detección de patrones.

3.3 Implementación de un laboratorio forense digital:

- Establecer un laboratorio equipado con tecnología de punta para análisis de evidencia digital.
- Capacitar al personal en el uso de las nuevas herramientas.

4. Mejora de la Cooperación Interinstitucional

4.1 Establecer protocolos de colaboración:

- Desarrollar acuerdos de cooperación con proveedores de servicios de internet y redes sociales.
- Crear canales de comunicación rápida con agencias internacionales de cibercrimen.

4.2 Implementar una plataforma de intercambio de información:

- Desarrollar una plataforma segura para compartir datos y evidencias con otras jurisdicciones.
- Establecer protocolos claros para el intercambio de información respetando las normativas de privacidad.

5. Programa de Prevención y Concientización

5.1 Campañas de educación pública:

- Desarrollar materiales educativos sobre ciberseguridad para diferentes grupos de edad.
- Implementar campañas en redes sociales y medios tradicionales.

5.2 Colaboración con instituciones educativas:

- Establecer programas de concientización sobre cibercrimen en escuelas y universidades.

- Ofrecer talleres y charlas por parte de expertos de la Fiscalía.

6. Monitoreo y Evaluación

6.1 Establecer indicadores de desempeño:

- Desarrollar métricas para evaluar la eficacia de las nuevas medidas implementadas.

- Realizar revisiones trimestrales del progreso.

6.2 Feedback continuo:

- Implementar un sistema de retroalimentación para el personal de la Fiscalía.

- Realizar encuestas anuales para medir la percepción pública sobre la seguridad cibernética.

Este plan de implementación aborda las principales áreas de mejora identificadas en el análisis, con un enfoque en la actualización legal, el fortalecimiento de recursos humanos y tecnológicos, y la mejora de la cooperación interinstitucional. La implementación gradual de estas medidas debería contribuir significativamente a mitigar el impacto del cibercrimen en la sociedad salteña y mejorar la capacidad de respuesta de la Fiscalía Especializada en Ciberdelitos.

DISCUSION

El cibercrimen representa un desafío creciente para las instituciones de justicia en todo el mundo, y la provincia de Salta, Argentina, no es una excepción. Esta discusión analiza la situación actual de la lucha contra el cibercrimen en Salta, basándose en entrevistas realizadas a miembros clave de la Fiscalía Especializada en Ciberdelitos y en datos estadísticos recientes de la región.

El análisis se centra en cinco áreas principales: la efectividad del marco legal vigente, los desafíos específicos en la persecución del cibercrimen, las fortalezas identificadas en la Fiscalía, las áreas que requieren mejora, y la importancia de la capacitación y los recursos tecnológicos. Además, se examinan casos de estudio locales, incluyendo el grooming, las estafas virtuales y el sexting, que ilustran la complejidad y la urgencia de los problemas enfrentados.

A lo largo de la discusión, se contrastan las experiencias y perspectivas locales con tendencias y estudios globales en ciberseguridad, proporcionando un contexto más amplio para entender los desafíos y las posibles soluciones en la lucha contra el cibercrimen en Salta. Este enfoque permite no solo identificar los problemas específicos de la región, sino también situar estos desafíos dentro del panorama más amplio de la ciberseguridad internacional.

La integración de datos locales con perspectivas globales busca ofrecer una visión comprehensiva de la situación actual, destacando tanto los avances logrados como las áreas que requieren atención urgente. Este análisis pretende ser una herramienta valiosa para informar futuras políticas y estrategias en la lucha contra el cibercrimen en Salta y, potencialmente, en otras regiones que enfrentan desafíos similares.

1. Efectividad del Marco Legal:

La Dra. Sofía Cornejo, Fiscal Especializada en Ciberdelitos, señaló que el marco legal actual ha avanzado, pero sigue enfrentando desafíos importantes debido a la rápida evolución de la tecnología y las tácticas de los ciberdelincuentes. Ella afirmó: "Para mitigar el impacto del cibercrimen en la sociedad, es crucial no solo actualizar la legislación de manera más ágil, sino también mejorar la coordinación entre las diferentes jurisdicciones y capacitar continuamente a los operadores de justicia".

Esta perspectiva se ve respaldada por los datos de Salta, donde se ha observado un aumento significativo en diversos tipos de ciberdelitos. Por ejemplo, según la Fiscalía

Especializada en Ciberdelitos de Salta (2023), se ha registrado un aumento del 30% en las denuncias por grooming en los últimos dos años. Este incremento subraya la necesidad de una legislación más ágil y adaptable a las nuevas modalidades de cibercrimen.

La prevalencia del grooming en Salta refleja una tendencia global de aumento en los delitos cibernéticos contra menores. Según un informe de UNICEF (2021), el confinamiento por la pandemia de COVID-19 ha exacerbado este problema a nivel mundial, aumentando la vulnerabilidad de los niños y adolescentes en línea.

La perspectiva de la Dra. Sofía Cornejo sobre la insuficiencia del marco legal actual frente al cibercrimen refleja un problema global en la legislación cibernética. Según un estudio de la UNODC (2013), la rápida evolución de la tecnología a menudo deja obsoletas las leyes existentes, creando vacíos legales que los ciberdelincuentes pueden explotar.

2. Desafíos en la Persecución del Cibercrimen:

Un desafío recurrente mencionado es la dificultad para rastrear a los delincuentes, especialmente cuando utilizan tecnologías como la red Tor, que enmascaran su ubicación. Según el Sumariante entrevistado, "la identificación de ciberdelincuentes que utilizan técnicas avanzadas como redes anónimas o encriptación es uno de los aspectos más desafiantes de nuestro trabajo".

En Salta, este desafío se manifiesta en la creciente sofisticación de las estafas virtuales. La Policía Cibernética de Salta ha reportado un incremento alarmante del 45% en denuncias por estafas virtuales durante el último año, con pérdidas económicas estimadas en varios millones de pesos (Policía de Salta, División de Delitos Tecnológicos, 2023). Estas estafas incluyen modalidades como el phishing, las estafas románticas y los fraudes de compra-venta en línea, que a menudo utilizan técnicas avanzadas de ocultamiento.

El incremento en las estafas virtuales en Salta es consistente con las tendencias globales. Un informe de la Asociación de Examinadores de Fraude Certificados (ACFE, 2022) señala que las estafas en línea han aumentado significativamente en todo el mundo, aprovechando la creciente dependencia de las transacciones digitales.

La dificultad para rastrear a los ciberdelincuentes que utilizan tecnologías de anonimización es un problema bien documentado en la literatura sobre ciberseguridad. Según un informe de Europol (2020), el uso de redes anónimas como Tor ha aumentado significativamente entre los ciberdelincuentes, dificultando la labor de las fuerzas del orden.

3. Fortalezas de la Fiscalía:

Una de las principales fortalezas de la Fiscalía radica en su especialización y el enfoque colaborativo entre su equipo. La Dra. Cornejo destacó que "la dedicación exclusiva al cibercrimen nos permite profundizar en cada caso y seguir las tendencias delictivas".

Esta especialización ha permitido a la Fiscalía de Salta abordar casos complejos como el grooming, que requiere un entendimiento profundo de las tácticas utilizadas por los depredadores en línea. La capacidad de la Fiscalía para identificar y perseguir estos casos ha sido crucial, considerando el aumento del 30% en denuncias por grooming en los últimos dos años (Fiscalía Especializada en Ciberdelitos de Salta, 2023).

La especialización y el enfoque colaborativo destacados por la Dra. Cornejo son consistentes con las mejores prácticas recomendadas por expertos en ciberseguridad. Según un informe del Foro Económico Mundial (2020), la especialización de las unidades de cibercrimen es crucial para hacer frente a la creciente sofisticación de los ciberdelincuentes.

4. Áreas de Mejora:

A pesar de las fortalezas identificadas, hay áreas que requieren mejoras significativas. La Dra. Cornejo mencionó la necesidad de "incorporar más tecnología avanzada para la investigación digital y fortalecer la cooperación interinstitucional".

En Salta, esta necesidad se hace evidente en casos como el sexting, donde la rápida difusión de contenido íntimo requiere una respuesta ágil y tecnológicamente avanzada. El Observatorio de Delitos Informáticos de Salta (2022) indica que el 20% de los adolescentes entre 14 y 17 años ha practicado sexting al menos una vez, lo que subraya la necesidad de herramientas tecnológicas más avanzadas para la detección y prevención.

La prevalencia del sexting entre los adolescentes de Salta refleja una tendencia observada en estudios internacionales. Una investigación publicada en JAMA Pediatrics (2019) encontró tasas similares de sexting entre adolescentes en varios países, subrayando la necesidad de abordar este fenómeno a nivel global.

La necesidad de incorporar tecnología avanzada y fortalecer la cooperación interinstitucional es un tema recurrente en la literatura sobre ciberseguridad. Un estudio de la RAND Corporation (2019) sugiere que la inversión en tecnologías de análisis forense digital y herramientas de inteligencia artificial puede mejorar significativamente la capacidad de las agencias de seguridad para combatir el cibercrimen.

5. Capacitación y Recursos Tecnológicos:

Todos los entrevistados coincidieron en la importancia de la capacitación continua y la necesidad de más recursos tecnológicos especializados. El Fiscal Auxiliar indicó que "la incorporación de más recursos humanos con formación especializada, como analistas de ciberseguridad, sería muy beneficiosa".

Esta necesidad se refleja en la complejidad de los casos que se manejan en Salta. Por ejemplo, para abordar eficazmente las estafas virtuales, que han aumentado un 45% en el último año (Policía de Salta, División de Delitos Tecnológicos, 2023), se requiere personal altamente capacitado en técnicas de investigación digital y análisis forense.

La unanimidad entre los entrevistados sobre la importancia de la capacitación continua y la necesidad de más recursos tecnológicos especializados refleja una tendencia global. Un informe de Gartner (2021) predice un aumento significativo en la inversión en tecnologías de ciberseguridad y capacitación especializada en los próximos años, reconociendo su papel crucial en la lucha contra el cibercrimen.

Las perspectivas y desafíos identificados por los entrevistados de la Fiscalía Especializada en Ciberdelitos de Salta son consistentes con las tendencias y problemas globales en la lucha contra el cibercrimen. Los datos específicos de Salta, como el aumento en casos de grooming, estafas virtuales y sexting, subrayan la urgencia de implementar mejoras en el marco legal, la cooperación interinstitucional, la tecnología y la capacitación especializada. Estas mejoras son esenciales para hacer frente a la creciente sofisticación y prevalencia de los ciberdelitos en la región.

CONCLUSIÓN

Mediante el trabajo de investigación de esta tesis se procuró analizar sobre el modo en que los delitos informáticos se encuentran regulados en la Argentina y más específicamente en la provincia de Salta, por lo tanto, la presente se denomina **"El Derecho como política contra el cibercrimen"**

Como se planteó al inicio de la presente, en la era digital, el cibercrimen emergió como una amenaza significativa para la seguridad ciudadana y la estabilidad social, desafiando los marcos legales tradicionales y exigiendo una adaptación rápida de las instituciones jurídicas.

El cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos.

Los delitos informáticos se encuentran en un proceso de expansión que se ha visto favorecido por la rápida y constante evolución de las tecnologías de la información y la comunicación.

Sobre la base de lo antedicho, en lo que sigue se procuró trazar un sobrevuelo en relación a la legislación vigente en Argentina y en Salta y también en países vecinos en materia de delitos informáticos.

El análisis de la efectividad del marco legal y las políticas contra el cibercrimen en Salta, con énfasis en la labor de la Fiscalía Especializada en Ciberdelitos, revela tanto avances significativos como desafíos persistentes en la lucha contra esta forma de delincuencia en constante evolución.

A través de mi investigación, busque recorrer primordialmente, el nuevo escenario objeto de comisión delitos, a consecuencia del avance de la tecnología y tratar de reconocer en las leyes lo que se encuentra en vigencia para luego empezar identificar las herramientas necesarias existentes en normativa.

En cuanto a la eficacia de la normativa vigente, se observa que, si bien el marco legal actual ha logrado avances, aún enfrenta limitaciones significativas. La Ley 26.388 de Delitos Informáticos ha proporcionado una base para abordar ciertos ciberdelitos, pero la rápida evolución de la tecnología y las tácticas de los ciberdelincuentes a menudo dejan obsoletas las leyes existentes.

El examen de la estructura y funcionamiento de la Fiscalía Especializada en Ciberdelitos de Salta revela fortalezas importantes, particularmente en su enfoque especializado y colaborativo. La dedicación exclusiva al cibercrimen ha permitido a la Fiscalía profundizar en casos complejos y seguir las tendencias delictivas emergentes. Sin embargo, también se identificaron áreas de mejora, especialmente en la necesidad de incorporar más

tecnología avanzada para la investigación digital y fortalecer la cooperación interinstitucional. Estos aspectos son cruciales para abordar de manera más efectiva delitos como el grooming, las estafas virtuales y el sexting, que han mostrado un aumento preocupante en la provincia.

Los avances constantes en materia tecnológica implican el surgimiento de nuevos paradigmas en informática, por lo tanto, aparece el término de una Sociedad de la Información, siendo un paradigma en el cual las tecnologías facilitan la creación, distribución y manipulación de la información y juegan un papel esencial en las actividades sociales, culturales y económicas.

Tales avances tecnológicos complejizan cada vez más la delimitación de las categorías dogmáticas de la conducta punible, como estructuras jurídicas que permitirían revelar mejor estas nuevas formas de criminalidad

Asimismo, y la luz de las leyes tratadas en la investigación es necesario señalar que todavía sigue siendo necesario implementar no solo leyes sino nuevas reglamentaciones que permitan reconocer y castigar al que cometa delitos en contra de las personas que se vulneran a través de estas, por lo tanto, es preciso y necesario una formación más específica tanto a legisladores como operadores de derecho.

La universalización de las redes sociales lleva y las nuevas formas de comunicación que se ven visibilizadas con el uso de internet aparecen también nuevas formas de delinquir y estas se tratan de tipificar en la legislación argentina y otras se encaminan a ser incluidas.

A modo de síntesis, de acuerdo a lo visto hasta el momento podemos decir que existe áreas que abordan la problemática del cibercrimen en términos prácticos; el Derecho y la seguridad informática.

Cada vez se hace más necesario continuar trabajando en materia legislativa sobre los delitos cibernéticos; así, existen varios proyectos de leyes que tratan nuevas figuras disvaliosas que no se encuentran tipificadas como delitos y por lo tanto no tienen asignado un castigo legal.

En conclusión, mientras la Fiscalía Especializada en Ciberdelitos de Salta ha demostrado fortalezas significativas en su enfoque especializado, es evidente que se requieren esfuerzos continuos para mitigar efectivamente el impacto del cibercrimen en la sociedad. La implementación de las estrategias propuestas, junto con una revisión y actualización constante del marco legal, será crucial para mejorar la capacidad de Salta para prevenir, investigar y perseguir los ciberdelitos de manera efectiva. Solo a través de un enfoque integral que combine legislación actualizada, recursos tecnológicos avanzados, personal altamente capacitado y colaboración interinstitucional, se podrá hacer frente a los desafíos cambiantes del cibercrimen en la provincia y proteger adecuadamente a sus ciudadanos en el entorno digital.

BIBLIOGRAFÍA

Área de Tecnología de la Información y de las Comunicaciones Aplicadas. (2011). Manual Básico de creación de páginas web. Creación de páginas webs. 1(1). https://www.um.es/atica/documentos/html.pdf

Asociación de Fiscales de Argentina. (2022). Informe sobre desafíos en la persecución de ciberdelitos en Argentina.

Bendinelli, M. (2014). Delitos informáticos. La importancia de la prueba digital en el proceso judicial. http://aldiaargentina.microjuris.com/2014/12/03/delitos-informaticos-la-importancia-de-la-prueba-digital-en-el-proceso-judicial/

Causa n° 46.744 "Fiscal s/ apela declaración de nulidad de informe pericial".

Causa Nº 135 "M. O., L. L. s/procesamiento Interlocutoria Sala de Feria "B" (17).- Juzgado de Instrucción Nº 30.

Concejo Deliberante de la Ciudad de Salta. (2017). Ordenanza N° 15.372.

Concejo Deliberante de la Ciudad de Salta. (2019). Ordenanza N° 15.789.

Concejo Deliberante de la Ciudad de Salta. (2021). Ordenanza N° 16.023.

Congreso de la Nación Argentina. (2008). Ley 26.388 de Delitos Informáticos.

Congreso de la Nación Argentina. (2017). Ley 27.411 de ratificación del Convenio de Budapest sobre Ciberdelincuencia.

Convención de Budapest. (2001).

Convención Sobre Los Derechos Del Niño, UNICEF. (2006).

Cuapio, M. R. (s.f.). Actualización judicial en el estado de Tlaxcala, dentro del marco del derecho informático y la informática jurídica en el siglo XXI. Marco Conceptual. http://www.ordenjuridico.gob.mx/Congreso/pdf/172.pdf

Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas. (2012).

División Contraterrorismo. (2015). Dirección Cibercrimen, Policía de la Provincia de Buenos Aires. Causa FLM 104/2014.

Dr. G. Ríos Patio. U.S.M.P. Facultad de Derecho, Revista Sapere. Delitos Electrónicos. http://www.derecho.usmp.edu.pe/instituto/revista/articulos/DELITOS_ELECTRONICOS.pdf

Dr. Montano Álvarez, A. A. (2008). La Problemática Jurídica en la Regulación de los Delitos Informáticos. http://www.ordenjuridico.gob.mx/Publicaciones/Tesis2010/01_LDP_MONTANO.pdf

Dupuy, D. T., Vaccarezza, M., Kiefer y C. Neme. (2012). Informe Final Cibercrimen C.A.B.A.

F.B.I. (2003). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

F.B.I. (2010). Internet Crime Schemes. www.fbi.gov/stats-services/publications/mortgage-fraud-2010

F.B.I. (2015). Internet Crime Complaint Center. www.fbi.gov/about-us/investigate/cyber

Fallo, de la Sala "M" de la Cámara Nacional de Apelaciones en lo Civil, "V., E. O. c/P., M. L. s/ divorcio art. 214 inc. 2do. Código Civil"

Fiscalía Especializada en Ciberdelitos de Salta. (2023). Informe Anual sobre Ciberdelitos en Salta.

García, J. (2015, 13 de noviembre). La informática, conceptos básicos y datos históricos. [Etimología]. http://lainformaticayelcomputador.blogspot.com.ar/

I.N.D.E.C. (2011). Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y de la Comunicación. Informe preliminar sobre indicadores básicos de acceso y uso. Resultados de mayo-julio de 2015. http://www.gobiernoabierto.gob.ar/multimedia/files/TICs_nacional.pdf

Khoo Boon Huim. (2012). Interpol le declara la guerra al cibercrimen, Fraude y Cibercrimen. https://haddensecurity.wordpress.com/2012/page/84/

Legislatura de la Provincia de Salta. (2019). Ley N° 8.186.

Ley 1.160/97, Delitos Informáticos, Paraguay. (1997).

Ley 1.768, Delitos Informáticos, Bolivia. (1997).

Ley 11.829, Delitos Informáticos, Brasil. (2008).

Ley 18168, Ley General de Telecomunicaciones, Chile. (2002).

Ley 19223, Delitos Informáticos, Chile. (1993).

Ley 20.009, Limita la Responsabilidad de los Usuarios De Tarjetas de Crédito por operaciones realizadas con Tarjetas Extraviadas, Hurtadas o Robadas. (2005).

Ley 25.326 Ley de Protección de Datos Personales. (2000). Argentina.

Ley 26.388 Ley de Delitos Informáticos. Argentina. (2008).

Ley 27.078 Tecnologías de la Información y las Comunicaciones. (2014).

Ley 27309, Delitos Informáticos. Perú. (2005).

Ley 863, Ley de Establecimiento Comerciales. (2003).

López, D. L. (s.f.). Protocolo de Actuaciones para Pericias Informáticas. Neuquén.

Lugo Ramírez, I. (s.f.). Introducción a las computadoras. Unidad de Servicios al Usuario (Vol. I). http://www.uprm.edu/cti/docs/manuales/manuales-espanol/vax-vms/manuales/Intcomp.pdf

Lujambio, I., Martínez, L., Rodríguez, E. y Fernández, C. (2005). Guía practica de internet. Acercando el uso de la Red a las Organizaciones Comunitarias 2(1), 17-19.

Menalkiawn. (2013). Manual básico de Seguridad Informática para activistas. una guía para proteger nuestros ordenadores y a nosotras mismas hacer frente a la represión y extender una cultura de seguridad. http://mexico.indymedia.org/IMG/pdf/libro_manual_seguridad_informa_tica_activistas.pdf

Ministerio de Seguridad de la Provincia de Buenos Aires. (s.f.). Boletín Informativo Nº 61. http://www.mseg.gba.gov.ar/Boletin%20Informativo/ordenes/his_pdf/BoletinInformativoM,JyS2011/BI-61-11.ACTUAL.pd72

Ministerio Público de Salta. (2020). Estructura y funciones de la Unidad Fiscal Especializada en Ciberdelitos.

Muller, E. (2015). Internacional. La NSA se prepara para la guerra mundial cibernética, según Der Spiegel. http://internacional.elpais.com/internacional/2015/01/17/actualidad/1421500678_347192.html

Observatorio de Delitos Informáticos de Salta. (2022). Estudio sobre Prácticas de Sexting en Adolescentes Salteños.

Paterlini N., Vega C., Guerriero G. y Velázquez M. (s.f.). Delitos Informáticos. Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos. http://www.aadat.org/delitos_informaticos20.htm

Poder Judicial de Salta. (2021). Reporte anual de actividades de la Fiscalía Especializada en Ciberdelitos.

Poder Judicial de Salta. (s.f.). Unidad Fiscal Especializada en Ciberdelitos.

Policía de Salta, División de Delitos Tecnológicos. (2023). Reporte Estadístico de Ciberdelitos en la Provincia.

Rivera, M. L. (2006-2007). Revista Jurídica. Obtenido de firma digital, consideraciones jurídicas: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20revista%20juridica/Revista%20Juridica%2006-07/articulos/02Firma.pdf

Sáenz, R. (2012). El problema de la investigación de los delitos informáticos. Revista Digital, El Derecho Informático.

Sáenz, R. (2012). Panorama del combate contra el Ciberdelito. Red Iberoamericana El Derecho Informático.

Saín, G. (1994). Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos. Argentina, Rustica.

Libro Segundo, Título XXVI.21

Proyecto de nuevo Código Penal, art. 502

Informe de gestión 2020 de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación–Argentina–, disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe.

Ley 30963 del 17 de junio de 2019-C P. Perú.

Informática y Delito. Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal AIDP - 1ª ed. - agosto/2014

Dupuy, Daniela: "La posesión de pornografía infantil", en AA.VV.: "Cibercrimen", bajo su propia dirección - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 139

Ley Nº 53-07. Delitos Informáticos. República Dominicana. (2007).

Ley 8/2011, Medidas para la Protección de las Infraestructuras Críticas. Jefatura del Estado, España. (2011).

Disposición Nº 2/2013, Jefatura de Gabinete de Ministros Secretaria de Gabinete y Coordinación Administrativa Subsecretaria de Tecnologías de Gestión Oficina Nacional de Tecnologías de Información.

Ag/res. 1939 (xxxiii-o/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética. (2003).

Ag/res. 1939 (xxxiii-o/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética resolución 2. (2003).

Ley N° 2861/06, Represión el comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces. (2006).

ANEXOS

Anexo I: Entrevistas

Entrevista con la Dra. Sofía Cornejo, Fiscal Especializada en Ciberdelitos

1: ¿Cómo evalúa la efectividad del marco legal actual en Salta para combatir el cibercrimen? ¿Qué mejoras cree que son necesarias para mitigar su impacto en la sociedad?

El marco legal actual en Salta ha avanzado en los últimos años, pero aún enfrenta desafíos significativos. Aunque contamos con normativas locales y nos alineamos con algunas internacionales, la rápida evolución de las tecnologías y las tácticas de los ciberdelincuentes nos exige una actualización constante. Para mitigar el impacto del cibercrimen en la sociedad, es crucial no solo actualizar la legislación de manera más ágil, sino también mejorar la coordinación entre las diferentes jurisdicciones y capacitar continuamente a los operadores de justicia.

2: ¿Considera que la normativa vigente a nivel local es suficiente para prevenir y perseguir el cibercrimen en Salta? ¿Cómo se compara esta normativa con la legislación internacional?

Si bien la normativa local ha sido eficaz en algunos aspectos, sigue siendo insuficiente para abordar todos los matices del cibercrimen. Comparada con la legislación internacional, nuestra normativa presenta lagunas que dificultan la persecución efectiva de estos delitos, especialmente en casos que trascienden fronteras. Es esencial que adoptemos prácticas internacionales y convenios que refuercen nuestra capacidad de respuesta.

3: ¿Cuáles son los tipos de cibercrimen más frecuentes en Salta y cómo aborda la Fiscalía su prevención y persecución?

En Salta, los cibercrímenes más frecuentes incluyen el grooming, las estafas virtuales y el sexting. La Fiscalía aborda estos delitos con un enfoque preventivo y reactivo, investigando casos con profundidad y colaborando con organismos nacionales e internacionales. Además, llevamos a cabo campañas de concientización para educar a la comunidad sobre los riesgos y las medidas de protección.

4: ¿Podría describir la estructura y el funcionamiento de la Fiscalía Especializada en Ciberdelitos de Salta? ¿Qué aspectos considera que son fortalezas en la lucha contra el cibercrimen?

La Fiscalía está compuesta por un equipo especializado que incluye dos auxiliares fiscales y ocho sumariantes, además de mí como fiscal titular. Una de nuestras mayores fortalezas es la dedicación exclusiva al cibercrimen, lo que nos permite profundizar en cada caso y seguir las tendencias delictivas. Además, el trabajo en equipo y la continua capacitación del personal son esenciales para mantenernos actualizados y ser efectivos.

5: ¿Qué desafíos enfrenta la Fiscalía en la persecución de delitos como grooming, estafas virtuales y sexting?

Los principales desafíos que enfrentamos son la rápida evolución tecnológica, la dificultad para rastrear a los delincuentes que actúan desde otras jurisdicciones y la falta de recursos suficientes para investigar a fondo cada caso. Además, la colaboración internacional es a menudo lenta, lo que complica la persecución de delitos transnacionales.

6: ¿Existen áreas de mejora dentro de la Fiscalía que podrían optimizar la lucha contra el cibercrimen?

Sin duda, la mejora continua es necesaria. Un área clave sería la incorporación de más tecnología avanzada para la investigación digital y el fortalecimiento de la cooperación interinstitucional. También es fundamental mejorar la capacitación del personal en nuevas técnicas de investigación y en el uso de herramientas específicas para combatir el cibercrimen.

7: ¿Qué importancia tiene la capacitación continua del personal en la Fiscalía Especializada en Ciberdelitos?

La capacitación continua es fundamental. El cibercrimen es un campo dinámico y en constante cambio, por lo que el personal debe estar siempre actualizado sobre las últimas tendencias, herramientas y métodos de investigación. La capacitación no solo mejora nuestras capacidades técnicas, sino que también aumenta la eficacia en la persecución de estos delitos.

8: ¿Cree que la incorporación de más recursos humanos y tecnológicos especializados podría mejorar la respuesta frente al cibercrimen en Salta? ¿Qué tipo de recursos considera prioritarios?

Absolutamente. La incorporación de más recursos humanos con formación especializada en cibercrimen, así como de herramientas tecnológicas avanzadas, es crucial para mejorar nuestra capacidad de respuesta. Prioritariamente, necesitamos software de última generación para análisis forense digital y plataformas que faciliten la cooperación internacional en tiempo real.

9: ¿Ha identificado la Fiscalía alguna necesidad particular de recursos o herramientas tecnológicas para mejorar su capacidad de respuesta frente al cibercrimen?

Sí, hemos identificado la necesidad de herramientas específicas para el análisis de datos en gran escala, así como software especializado en rastreo y monitoreo de actividades sospechosas en la web y la dark web. Además, contar con un laboratorio forense digital bien equipado sería un gran avance para mejorar nuestra capacidad de respuesta y resolver casos con mayor rapidez y precisión.

Entrevista con el Fiscal Auxiliar de la Fiscalía Especializada en Ciberdelitos de Salta

1: ¿Cómo evalúa la efectividad del marco legal actual en Salta para combatir el cibercrimen? ¿Qué mejoras cree que son necesarias para mitigar su impacto en la sociedad?

El marco legal en Salta ha mejorado considerablemente, pero aún presenta desafíos significativos. En la práctica, las leyes vigentes nos permiten actuar en varios casos, pero hay áreas donde la legislación es insuficiente, especialmente en lo que respecta a la rapidez de la respuesta y la cooperación internacional. Considero que es fundamental actualizar las normativas y promover una mayor especialización dentro del sistema judicial para que podamos ser más efectivos en la mitigación del cibercrimen.

2: ¿Cuáles son los principales retos que enfrenta la Fiscalía en la persecución de delitos como grooming, estafas virtuales y sexting?

Los principales retos incluyen la identificación de los perpetradores, que a menudo utilizan herramientas para ocultar su identidad y ubicación, como el uso de redes anónimas. Además, muchos de estos delitos son transnacionales, lo que complica la persecución debido a las diferencias en los marcos legales y la lentitud en la cooperación internacional. Otro desafío es la falta de recursos especializados para analizar y procesar grandes volúmenes de datos digitales.

3: ¿Cómo se organiza el trabajo en la Fiscalía para abordar los casos de cibercrimen?

La Fiscalía está organizada en equipos que se especializan en diferentes áreas del cibercrimen. Contamos con dos auxiliares fiscales que supervisan las investigaciones y coordinan con los sumariantes, quienes son responsables de la recopilación y análisis de evidencia digital. Trabajamos de manera muy colaborativa, lo que nos permite abordar los casos de manera integral y eficiente, aunque siempre estamos buscando formas de optimizar nuestros procesos.

4: ¿Qué considera que son las principales fortalezas de la Fiscalía en la lucha contra el cibercrimen?

Una de nuestras principales fortalezas es la especialización. Al estar dedicados exclusivamente al cibercrimen, hemos desarrollado una profunda comprensión de las particularidades de estos delitos. Además, nuestro equipo está en constante capacitación, lo que nos permite estar al día con las últimas tecnologías y métodos de investigación. La colaboración interna y con otras instituciones también es un punto fuerte que nos permite ser más efectivos.

5: ¿Existen áreas dentro de la Fiscalía que considera que necesitan mejoras?

Sin duda, siempre hay margen para mejorar. Una de las áreas clave que necesitamos fortalecer es la tecnología que utilizamos. Aunque contamos con herramientas adecuadas, la rápida evolución del cibercrimen requiere que tengamos acceso a las últimas tecnologías de

análisis y monitoreo. También sería beneficioso ampliar nuestro equipo con más especialistas en ciberseguridad y análisis forense digital.

6: ¿Qué importancia tiene la capacitación del personal en la Fiscalía Especializada en Ciberdelitos?

La capacitación es absolutamente crucial. El cibercrimen es un campo que cambia constantemente, con nuevas amenazas y técnicas emergiendo regularmente. Sin una capacitación continua, corremos el riesgo de quedarnos atrás y de ser menos efectivos en la persecución de estos delitos. Es por eso que invertimos tiempo y recursos en mantener a nuestro personal actualizado y en contacto con las últimas tendencias y herramientas en el campo.

7: ¿Considera que la incorporación de más recursos humanos y tecnológicos podría mejorar la capacidad de respuesta frente al cibercrimen en Salta?

Sí, definitivamente. La incorporación de más recursos humanos con formación especializada, como analistas de ciberseguridad y expertos en forense digital, sería muy beneficiosa. Además, la adquisición de tecnologías avanzadas, como software para el análisis de big data y herramientas de rastreo de actividades en la dark web, mejoraría considerablemente nuestra capacidad de respuesta y nos permitiría abordar los casos con mayor precisión y eficiencia.

8: ¿Qué tipo de herramientas tecnológicas cree que son prioritarias para mejorar la labor de la Fiscalía?

Prioritariamente, necesitamos herramientas que nos permitan realizar análisis forense de dispositivos de manera más rápida y eficaz. También sería muy útil contar con software de inteligencia artificial que nos ayude a identificar patrones en grandes volúmenes de datos y herramientas que faciliten la colaboración con otras jurisdicciones en tiempo real. Estas tecnologías no solo mejorarían nuestra eficiencia, sino que también aumentarían nuestras posibilidades de éxito en la persecución de delitos cibernéticos complejos.

Entrevista con un Sumariante de la Fiscalía Especializada en Ciberdelitos de Salta

1: ¿Cuáles son las tareas principales que realiza como sumariante en la Fiscalía Especializada en Ciberdelitos?

Mi labor principal como sumariante es la recopilación y análisis de pruebas digitales. Esto incluye extraer información de dispositivos electrónicos, analizar redes sociales, correos electrónicos, y cualquier otra plataforma digital que pueda estar involucrada en un delito. También preparo informes detallados que se utilizan en las investigaciones y en los procesos judiciales, asegurándome de que toda la evidencia sea obtenida y conservada de manera que sea admisible en los tribunales.

2: ¿Qué desafíos enfrenta en la recolección de evidencia digital en casos de cibercrimen?

Uno de los mayores desafíos es la encriptación de datos. Muchos ciberdelincuentes utilizan tecnologías avanzadas para proteger su información, lo que dificulta su acceso. Otro reto es la volatilidad de la evidencia digital, que puede ser modificada o eliminada rápidamente. Además, la colaboración con proveedores de servicios de internet o redes sociales a veces es complicada y puede llevar tiempo, lo cual puede retrasar las investigaciones.

3: ¿Qué tipo de capacitación ha recibido para llevar a cabo su trabajo?

He recibido capacitación en análisis forense digital, manejo de evidencias electrónicas, y técnicas de investigación en cibercrimen. También he participado en cursos específicos sobre nuevas tecnologías y herramientas de análisis de datos. La capacitación es continua, dado que el campo del cibercrimen evoluciona rápidamente, y es crucial estar al día con las últimas tendencias y tecnologías para realizar nuestro trabajo de manera eficaz.

4: ¿Cómo es el trabajo en equipo dentro de la Fiscalía, especialmente en la colaboración entre sumariantes y fiscales?

El trabajo en equipo es fundamental en la Fiscalía. Colaboramos estrechamente con los fiscales para asegurarnos de que toda la evidencia que recolectamos se alinee con los

requerimientos legales y pueda ser utilizada en los casos. Los fiscales nos orientan sobre los aspectos legales que debemos considerar, y nosotros les proporcionamos la información técnica necesaria para fortalecer las investigaciones. Esta sinergia es clave para el éxito en la persecución de delitos cibernéticos.

5: ¿Qué herramientas tecnológicas utiliza en su trabajo diario?

Utilizamos una variedad de herramientas tecnológicas, incluyendo software de análisis forense digital, herramientas para la recuperación de datos borrados, y programas de rastreo de actividades en línea. También usamos bases de datos y sistemas de inteligencia artificial para identificar patrones y conexiones entre diferentes casos. Estas herramientas son esenciales para realizar un análisis exhaustivo y preciso de la evidencia digital.

6: ¿Cuál es su experiencia en la identificación de ciberdelincuentes que utilizan técnicas avanzadas para ocultar su identidad?

La identificación de ciberdelincuentes que utilizan técnicas avanzadas, como redes anónimas o encriptación, es uno de los aspectos más desafiantes de nuestro trabajo. Requiere un análisis detallado de los datos y, a menudo, la colaboración con expertos en ciberseguridad. Hemos tenido que desarrollar métodos específicos para rastrear y desenmascarar a estos individuos, a veces trabajando en conjunto con otras agencias o empresas tecnológicas para lograrlo.

7: ¿Cómo evalúa la efectividad de los procedimientos actuales en la Fiscalía para enfrentar el cibercrimen?

Los procedimientos actuales son efectivos en muchos casos, pero siempre hay margen para mejorar. La rápida evolución del cibercrimen requiere que constantemente revisemos y actualicemos nuestros métodos y tecnologías. A veces nos encontramos con limitaciones tecnológicas o legales que pueden complicar la investigación, por lo que es crucial seguir innovando y adaptándonos a nuevas amenazas.

8: ¿Qué mejoras considera necesarias para optimizar su trabajo y el de la Fiscalía en general?

Sería beneficioso contar con más recursos humanos especializados, especialmente en áreas como la criptografía y el análisis de redes complejas. Además, la incorporación de tecnologías más avanzadas para el análisis forense digital y la detección de actividades sospechosas en tiempo real mejoraría significativamente nuestra capacidad de respuesta. Finalmente, una mayor colaboración con otras jurisdicciones y organismos internacionales también sería crucial, dado que muchos de los delitos que investigamos tienen un componente transnacional.