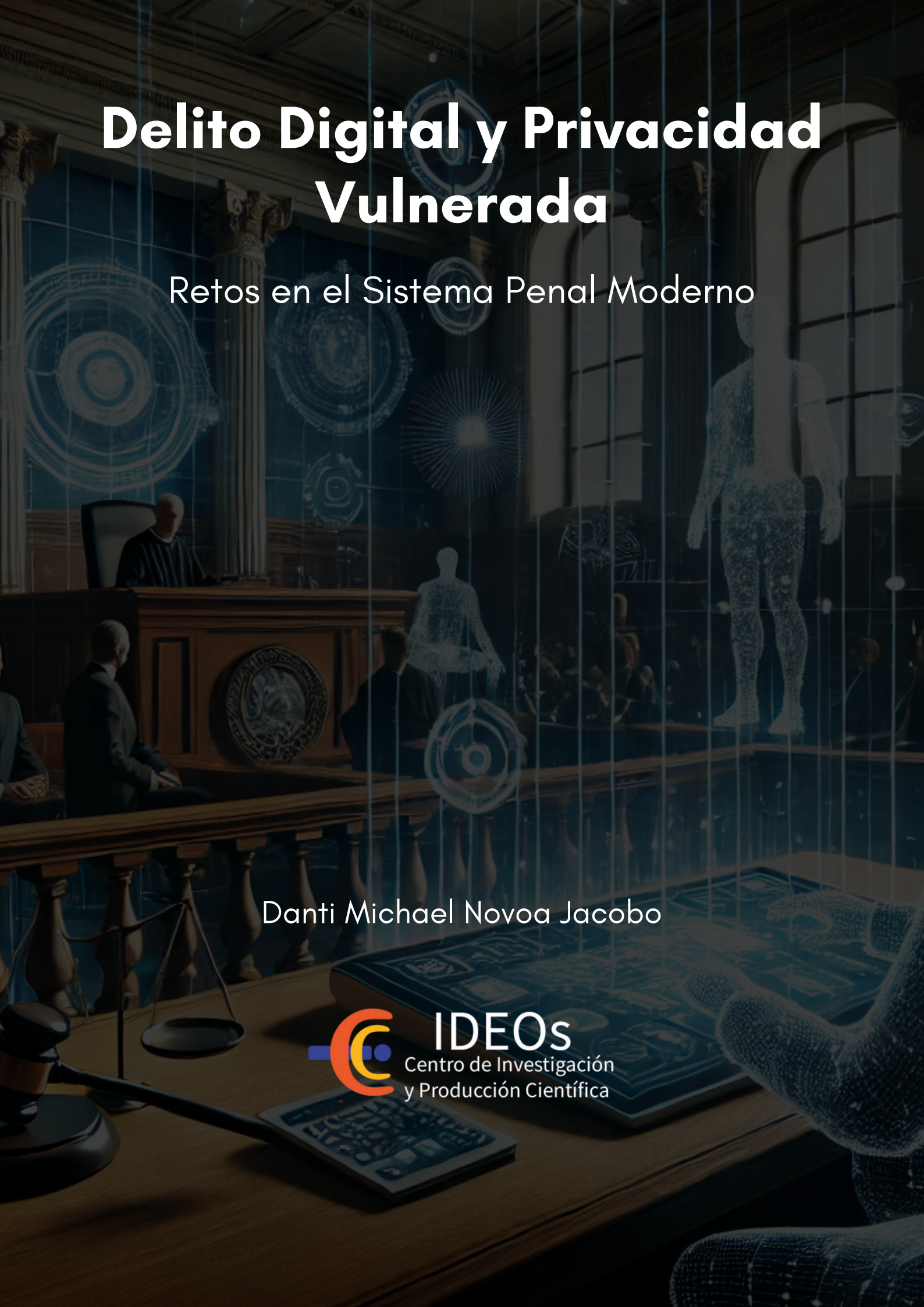


Delito Digital y Privacidad Vulnerada

Retos en el Sistema Penal Moderno

Danti Michael Novoa Jacobo

IDEOs
Centro de Investigación
y Producción Científica

Delito Digital y Privacidad Vulnerada

Retos en el Sistema Penal Moderno

Editor

IDEOs
Centro de Investigación
y Producción Científica

Delito Digital y Privacidad Vulnerada
Retos en el Sistema Penal Moderno

Danti Michael Novoa Jacobo

Editado por

CENTRO DE INVESTIGACIÓN & PRODUCCIÓN CIENTÍFICA IDEOS E.I.R.L

Dirección: Calle Teruel 292, Miraflores, Lima, Perú.

RUC: 20606452153

Primera edición digital, Enero 2025

Libro electrónico disponible en www.tecnohumanismo.online

ISBN: 978-612-5166-25-8

Registro de Depósito legal N°: 2025-00919

DEDICATORIA

A Dios, a mí amada esposa Carmen y a mis hermosas y adoradas hijitas, por ser el motor que impulsa cada día de mi vida. Los amo hasta el infinito.

A mis padres, Mariano y Luz Angélica, por ser las personas más influyentes en mi vida.

A Betty y Verónica, quienes estuvieron siempre a mi lado en las buenas y en las malas, sobre todo en el desarrollo de esta tesis.

Danti Michael

AGRADECIMIENTO

Agradezco a Dios por darme la oportunidad y fuerza necesaria para seguir adelante en esta ardua labor de cursar mis estudios de una segunda maestría y llevarla hasta el final.

A mi asesor, el Dr. Recalde Gracey, Andrés Enrique y a mis docentes de la Universidad Cesar Vallejo - Escuela de Posgrado, ya que ellos fueron la dirección de esta investigación.

Danti Michael

ÍNDICE

RESEÑA

En el contexto de una sociedad profundamente transformada por la tecnología de la información, este libro se presenta como una obra clave para entender los desafíos que enfrentan los sistemas de justicia en la era digital. La investigación que sustenta el texto aborda una problemática fundamental: ¿cómo impacta el uso de sistemas y datos informáticos en la transgresión del derecho a la intimidad dentro del ámbito judicial? Desde esta perspectiva, la obra explora en profundidad cómo las herramientas tecnológicas, esenciales para la modernización y eficiencia de la administración de justicia, pueden convertirse también en fuentes de vulneración de derechos fundamentales.

El análisis se centra específicamente en el entorno de un Juzgado Unipersonal en el año 2022. La investigación parte de una hipótesis clara y audaz: el injusto penal vinculado a los sistemas y datos informáticos tiene una incidencia significativa en la violación del derecho a la intimidad. Para abordar esta cuestión, el autor o autora adopta un enfoque metodológico riguroso que combina el análisis cuantitativo, un diseño transversal no experimental y un enfoque correlacional. Este marco metodológico permite no solo analizar el problema desde una perspectiva teórica, sino también ofrecer evidencia empírica sólida que respalda las conclusiones alcanzadas.

El libro se destaca por la claridad y precisión con la que se presenta la investigación. La muestra incluyó a 30 profesionales del derecho, entre jueces, asistentes y secretarios, que desempeñan sus funciones en un Juzgado Unipersonal. A través de cuestionarios diseñados y validados por expertos, se recolectaron datos relevantes que permitieron evaluar la relación entre las variables en estudio. La alta confiabilidad de los instrumentos utilizados, con coeficientes alfa de Cronbach de 0,830 y 0,822, refuerza la credibilidad de los hallazgos obtenidos.

Los resultados presentados en el libro son reveladores. Las pruebas de hipótesis muestran una relación positiva alta entre el injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad, con un coeficiente de correlación de r = 0,630**. Además, el análisis de regresión lineal destaca que, en el contexto de un Juzgado Unipersonal, el injusto penal vinculado a la tecnología incide en un 70% sobre la variable que mide la vulneración del derecho a la intimidad. Estas cifras no solo confirman la

hipótesis inicial, sino que además subrayan la urgencia de abordar este fenómeno desde una perspectiva tanto jurídica como tecnológica.

A lo largo del libro, el autor combina con maestría la exposición teórica y los datos empíricos. Se analiza cómo los avances tecnológicos, si bien ofrecen beneficios innegables en términos de eficiencia y acceso a la justicia, también generan nuevos riesgos y desafíos éticos para el sistema judicial. El texto examina, entre otros aspectos, el papel de la protección de datos, la confidencialidad de la información judicial y el equilibrio entre la transparencia y la privacidad en la era digital. Este análisis se complementa con propuestas concretas que buscan mitigar los riesgos y fortalecer el marco normativo en torno al uso de la tecnología en los procesos judiciales.

El libro no solo es una contribución valiosa al ámbito académico, sino que también tiene un profundo impacto práctico. Las conclusiones y recomendaciones que se desprenden de la investigación son altamente relevantes para legisladores, jueces, abogados, tecnólogos y todos aquellos involucrados en el diseño de políticas públicas en el ámbito de la justicia. Además, el texto invita a reflexionar sobre la necesidad de un enfoque multidisciplinario que integre conocimientos del derecho, la tecnología y la ética para garantizar una administración de justicia equitativa y respetuosa de los derechos humanos en el entorno digital.

En definitiva, esta obra se posiciona como un referente indispensable para quienes buscan entender y abordar los complejos desafíos que surgen en la intersección entre la tecnología y el derecho. Con un estilo accesible pero profundamente fundamentado, el autor o autora ofrece un análisis detallado y esclarecedor que no solo ilumina el problema, sino que también apunta hacia soluciones viables y necesarias. Este libro es, sin duda, una contribución significativa para el desarrollo de un sistema de justicia más justo y adaptado a los retos del siglo XXI.

CAPÍTULO I

MARCO TEÓRICO

El marco teórico constituye una de las partes fundamentales de cualquier investigación, ya que proporciona el contexto necesario para comprender los conceptos clave, teorías y enfoques que sustentan el estudio. En este capítulo, se busca presentar y analizar las principales teorías y antecedentes que sirven como base para el desarrollo de la investigación. Además, se abordarán las definiciones y los enfoques más relevantes que permiten contextualizar el objeto de estudio, establecer las relaciones entre los distintos conceptos y señalar las brechas o áreas que serán exploradas a lo largo del trabajo.

Este capítulo tiene como objetivo proporcionar al lector un marco conceptual que le permita comprender las discusiones y hallazgos que se desarrollarán en los capítulos posteriores, contextualizando la importancia del tema dentro del campo de estudio y resaltando las principales perspectivas que guiarán la investigación.

1.1. Fundamentos Conceptuales y Teóricos

1.1.1. Concepto de Injusto Penal

El concepto de injusto penal se refiere a la acción u omisión que contraviene el orden jurídico penal, causando un daño o peligro a un bien jurídico protegido. En este marco, el injusto penal no solo se enfoca en el acto ilícito como tal, sino también en el reproche social y jurídico que conlleva. Esta figura se constituye a partir de tres elementos esenciales: la tipicidad, la antijuridicidad y la culpabilidad.

- **Tipicidad:** Refiere a la correspondencia entre la conducta delictiva y lo descrito en el tipo penal. En el contexto de sistemas y datos informáticos, la tipicidad incluye actos como el acceso indebido, la manipulación de datos personales o el uso de sistemas tecnológicos para fines ilícitos.

- **Antijuridicidad:** Analiza si la conducta tipificada contraviene un bien jurídico protegido. En el ámbito de la tecnología, el derecho a la intimidad

emerge como un bien jurídico especialmente vulnerable debido a la capacidad de los sistemas para recopilar, almacenar y manipular grandes volúmenes de datos personales.

- **Culpabilidad:** Este elemento evalúa el grado de reprochabilidad del sujeto que comete el delito. En los casos de delitos informáticos, la culpabilidad puede complicarse por factores como la intención, la negligencia y el conocimiento técnico del infractor.

En el ámbito judicial, el injusto penal relacionado con sistemas informáticos adquiere una dimensión compleja debido a la rapidez con la que evolucionan las tecnologías, las lagunas normativas existentes y la dificultad para identificar responsables en delitos transfronterizos.

1.1.2. Principios del Derecho a la Intimidad

El derecho a la intimidad es un principio fundamental que garantiza a los individuos la protección frente a injerencias indebidas en su vida privada. Reconocido en múltiples instrumentos jurídicos internacionales, como el **Pacto Internacional de Derechos Civiles y Políticos (artículo 17)** y la **Convención Americana sobre Derechos Humanos (artículo 11)**, este derecho es esencial para salvaguardar la dignidad humana en la era digital.

- **Protección de la vida privada:** Incluye el resguardo de información personal, familiar, profesional y social frente a la divulgación o uso sin consentimiento. En el contexto judicial, esto implica que los sistemas que manejan datos de las partes involucradas deben garantizar la confidencialidad.

- **Autonomía informativa:** Este principio faculta a los individuos a controlar el uso de sus datos personales. Sin embargo, en el ámbito judicial, este principio puede entrar en conflicto con la necesidad de transparencia en los procesos legales.

- **Proporcionalidad y finalidad:** El derecho a la intimidad no es absoluto y puede limitarse en casos donde el interés público lo exija. No obstante,

estas limitaciones deben ser proporcionales y estar orientadas a un fin legítimo, como la persecución del delito o la resolución de conflictos judiciales.

En el entorno de los sistemas informáticos, la implementación de medidas de seguridad robustas y el cumplimiento de normativas como el **Reglamento General de Protección de Datos (GDPR)** son fundamentales para preservar estos principios.

1.1.3. La Tecnología como Herramienta y Amenaza en el Ámbito Judicial

La tecnología ha revolucionado el funcionamiento de los sistemas judiciales, facilitando procesos y mejorando el acceso a la justicia. Sin embargo, su implementación también plantea riesgos significativos para los derechos fundamentales, especialmente el derecho a la intimidad.

Tecnología como herramienta:

- **Automatización de procesos:** Sistemas como los expedientes digitales y las audiencias virtuales han optimizado la eficiencia en los juzgados.
- **Acceso a la información:** Las bases de datos judiciales permiten a las partes involucradas acceder a documentos y evidencia de manera rápida y segura.
- **Transparencia:** Los sistemas de monitoreo y seguimiento de casos fortalecen la rendición de cuentas en los procesos legales.

Tecnología como amenaza:

- **Vulnerabilidades en la seguridad:** Los sistemas judiciales que manejan datos personales están expuestos a ataques cibernéticos, como hackeos o filtraciones de información.
- **Injerencia indebida:** El acceso no autorizado a información confidencial puede derivar en la vulneración de derechos fundamentales, como la intimidad de las partes involucradas.

- **Uso indebido de datos:** Las tecnologías de análisis masivo de datos pueden ser utilizadas para fines discriminatorios o contrarios a los derechos humanos.

El reto principal radica en equilibrar los beneficios de la tecnología con la necesidad de proteger los derechos fundamentales. Esto implica adoptar medidas como:

- El uso de herramientas tecnológicas con altos estándares de seguridad.
- Capacitación del personal judicial en el manejo ético de los sistemas informáticos.
- Implementación de marcos normativos claros que delimiten el uso de la tecnología en los procesos legales.

En conclusión, el marco conceptual y teórico de esta sección proporciona los fundamentos necesarios para comprender el impacto del injusto penal relacionado con sistemas y datos informáticos en la transgresión del derecho a la intimidad. Este análisis establece las bases para profundizar en los aspectos prácticos y normativos que se desarrollan en los capítulos siguientes.

1.2. El contexto jurídico en la era digital

La rápida evolución de la tecnología ha transformado numerosos aspectos de la vida cotidiana, y el ámbito jurídico no ha quedado exento de estos cambios. En la actualidad, los avances tecnológicos impactan de manera profunda en los sistemas judiciales, el manejo de datos personales y la protección de los derechos fundamentales, entre ellos el derecho a la intimidad. Este capítulo analiza cómo la tecnología ha modificado el panorama jurídico, especialmente en términos de procesos judiciales, regulaciones sobre la protección de datos y los riesgos asociados con la vulneración de la intimidad.

1.2.1. Impacto de la tecnología en los sistemas judiciales

La incorporación de la tecnología en los sistemas judiciales ha transformado tanto la administración de justicia como la forma en que los litigios son resueltos. A través de

herramientas como la digitalización de documentos, el uso de inteligencia artificial para la predicción de fallos, y la implementación de tribunales virtuales, los sistemas judiciales han logrado mejorar la eficiencia en el manejo de los casos, la reducción de tiempos de espera y la democratización del acceso a la justicia.

Por ejemplo, el uso de plataformas digitales para presentar demandas, audiencias virtuales o el acceso remoto a bases de datos judiciales ha permitido que los procesos legales sean más ágiles y accesibles, especialmente en situaciones donde los tribunales se encuentran saturados o donde las distancias geográficas representan una barrera para el acceso físico a la justicia. A su vez, la automatización de ciertos procedimientos ha reducido la carga administrativa, permitiendo que los recursos humanos del sistema judicial puedan enfocarse en tareas más complejas.

Sin embargo, la adopción de la tecnología también presenta desafíos significativos, entre los cuales destacan la necesidad de garantizar la ciberseguridad, evitar la manipulación de pruebas electrónicas, y asegurar que los derechos fundamentales de los involucrados sean respetados en un entorno digital. El uso indebido de tecnologías como el reconocimiento facial o los algoritmos de predicción también ha generado preocupación sobre el respeto a los derechos de los ciudadanos en el proceso judicial.

1.2.2. Regulaciones legales en el manejo de datos informáticos

El manejo de datos informáticos es una de las áreas más afectadas por los avances tecnológicos. La recopilación, almacenamiento y procesamiento de grandes volúmenes de datos, particularmente aquellos que contienen información sensible, como los datos personales, de salud o financieros, ha suscitado un debate sobre la necesidad de regulaciones más estrictas para proteger los derechos de los individuos.

En muchos países, la regulación del uso de datos informáticos está comenzando a tomar forma a través de leyes específicas, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, o la Ley de Protección de Datos Personales en diversas naciones. Estas regulaciones buscan asegurar que las entidades que manejan datos personales actúen con transparencia, respeto y responsabilidad, implementando medidas para la protección de la privacidad y el consentimiento informado.

A nivel global, existen diferentes enfoques regulatorios para el manejo de los datos informáticos. En algunos lugares, las leyes están orientadas a dar a los individuos el control sobre sus datos, permitiendo que puedan acceder a la información que se posee sobre ellos, corregirla o solicitar su eliminación. En otros, la regulación se centra más en las sanciones a las empresas que no cumplan con las normativas, imponiendo multas millonarias.

La creciente preocupación por la privacidad también ha llevado a una revisión del marco jurídico relacionado con el almacenamiento y la transferencia internacional de datos. Este contexto es clave para abordar la seguridad cibernética y la prevención de delitos informáticos, como el robo de identidad, el hacking o el uso indebido de información personal.

1.2.3. Casos emblemáticos de vulneración del derecho a la intimidad

En la era digital, los casos de vulneración del derecho a la intimidad se han multiplicado, reflejando la tensión entre la privacidad individual y las necesidades de las empresas y gobiernos en un entorno cada vez más conectado. Uno de los casos emblemáticos más conocidos fue el escándalo de Cambridge Analytica, donde millones de datos de usuarios de Facebook fueron recogidos sin su consentimiento explícito para ser utilizados en campañas políticas. Este caso reveló la magnitud de la recopilación de datos personales y la manipulación de información en la esfera pública, lo que generó un debate global sobre el alcance de la privacidad en plataformas digitales.

Otro caso importante en la vulneración del derecho a la intimidad involucró el acceso no autorizado a dispositivos móviles, como el caso de los "Fappening", en el que se filtraron fotos íntimas de celebridades, evidenciando cómo las tecnologías de la información pueden ser utilizadas para invadir la privacidad personal. Estos incidentes subrayan la vulnerabilidad de los individuos frente a las tecnologías de almacenamiento y transmisión de datos, y el potencial de las plataformas digitales para acceder a información personal sin el consentimiento de sus titulares.

Los casos de vigilancia masiva también han sido puntos de controversia. La revelación de programas de espionaje como los destapados por Edward Snowden, en los cuales gobiernos recopilan indiscriminadamente datos de ciudadanos, ha generado un

debate sobre la legitimidad y el alcance de las políticas de seguridad nacional y su colisión con los derechos de privacidad.

En respuesta a estos incidentes, los legisladores han buscado desarrollar leyes que fortalezcan la protección del derecho a la intimidad en el ámbito digital. Sin embargo, la falta de armonización entre las regulaciones internacionales y la rapidez con que avanzan las tecnologías siguen siendo barreras para una protección efectiva. Esto plantea la necesidad de contar con marcos legales que se adapten a la dinámica de la digitalización y que, a su vez, aseguren la salvaguarda de los derechos fundamentales en el mundo virtual.

En la era digital, el contexto jurídico debe evolucionar rápidamente para hacer frente a los nuevos retos planteados por la tecnología. La transformación de los sistemas judiciales, el manejo de datos informáticos y la protección del derecho a la intimidad son aspectos clave en este proceso. A medida que la tecnología avanza, es esencial que las regulaciones y políticas jurídicas se adapten para garantizar que los derechos fundamentales de los individuos sean respetados, asegurando que la digitalización no se convierta en un obstáculo para la justicia, la privacidad y la equidad.

1.3. Derecho a la intimidad y su protección

El derecho a la intimidad es uno de los derechos fundamentales más importantes en el marco de las libertades individuales y la protección de la dignidad humana. En la era digital, este derecho ha adquirido una relevancia aún mayor, dado el avance de las tecnologías de la información y la comunicación, que han facilitado el acceso y la circulación de datos personales de manera masiva. La protección de la intimidad se ha convertido en un desafío crucial para los sistemas jurídicos, que deben equilibrar la necesidad de seguridad y transparencia con la preservación de los derechos individuales. Este capítulo aborda la definición y alcance del derecho a la intimidad, los instrumentos legales que lo protegen tanto a nivel internacional como local, y los desafíos que enfrenta en el contexto digital.

1.3.1. Definición y alcance del derecho a la intimidad

El derecho a la intimidad se define como el derecho de cada individuo a decidir qué información personal, que pertenece exclusivamente a su vida privada, puede ser divulgada a otros, y en qué condiciones. Este derecho está estrechamente relacionado con la dignidad humana, la libertad personal y la protección de la privacidad. En su sentido más amplio, abarca diversos aspectos de la vida privada, como la familia, el hogar, la correspondencia y las comunicaciones, y se extiende a la protección de la imagen, la reputación y la información personal.

En términos jurídicos, el derecho a la intimidad puede ser entendido como una defensa frente a la invasión no autorizada de la esfera personal por parte de terceros, ya sean estos individuos, empresas o instituciones. Su alcance incluye tanto la protección contra la obtención de información personal sin el consentimiento del individuo, como la restricción en la difusión de dicha información, independientemente de su veracidad. Esto implica que, incluso cuando la información es correcta, su revelación no autorizada puede constituir una vulneración del derecho a la intimidad.

En el contexto de la era digital, el alcance del derecho a la intimidad se ha expandido y diversificado. Las redes sociales, las plataformas de comercio electrónico, las aplicaciones móviles y otras tecnologías han creado nuevos espacios en los que la privacidad de los individuos puede ser fácilmente comprometida. La recopilación masiva de datos personales a través de internet y la interconexión de dispositivos han generado situaciones en las que la intimidad de las personas se ve amenazada constantemente.

1.3.2. Instrumentos legales internacionales y locales

A lo largo de los años, se han desarrollado una serie de instrumentos legales, tanto internacionales como locales, para garantizar la protección del derecho a la intimidad. Estos instrumentos buscan establecer un marco jurídico que regule la recolección, el almacenamiento, el uso y la difusión de la información personal, buscando garantizar el respeto a la privacidad de los individuos.

A nivel internacional, uno de los instrumentos clave es el **Pacto Internacional sobre Derechos Civiles y Políticos (PIDCP)**, adoptado por la Asamblea General de la

ONU en 1966, que establece en su artículo 17 la protección del derecho a la intimidad. Este pacto garantiza a todas las personas el derecho a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia.

En la Unión Europea, la **Carta de los Derechos Fundamentales de la Unión Europea** también contempla el derecho a la intimidad, especialmente en su artículo 7, que establece el respeto a la vida privada y familiar, el hogar y la comunicación. A nivel europeo, el **Reglamento General de Protección de Datos (GDPR)** se ha convertido en una de las normativas más estrictas y avanzadas en la protección de la privacidad, imponiendo reglas claras sobre el manejo de datos personales y otorgando a los individuos el control sobre sus propios datos.

En América Latina, muchos países han adoptado leyes que buscan proteger el derecho a la intimidad, como la **Ley de Protección de Datos Personales** en varios países, que establece normas sobre cómo las empresas y organizaciones deben manejar la información personal de los ciudadanos. En algunos países como Argentina y Brasil, la legislación ha avanzado considerablemente en este aspecto, impulsando regulaciones que se asemejan al GDPR europeo, con un enfoque en la transparencia, el consentimiento y la seguridad de los datos personales.

A nivel local, cada país tiene su propio marco legal en función de sus necesidades y circunstancias particulares. Estos marcos legales incluyen la legislación sobre privacidad y protección de datos, que exige que las empresas y las instituciones obtengan el consentimiento explícito de los individuos para el uso de sus datos personales y que implementen medidas adecuadas de seguridad para protegerlos. Las leyes nacionales también suelen incorporar mecanismos de reparación en caso de vulneración de este derecho, como la posibilidad de presentar reclamaciones ante autoridades de protección de datos.

1.3.3. Desafíos en la protección de la intimidad en la era digital

La protección del derecho a la intimidad en la era digital enfrenta una serie de desafíos que complican su aplicación y refuerzan la necesidad de un marco legal dinámico que se adapte rápidamente a los avances tecnológicos. Uno de los principales retos es el volumen y la naturaleza de los datos personales que se recopilan y procesan en la

actualidad. Las plataformas digitales, aplicaciones móviles y redes sociales recopilan constantemente datos sobre las personas, desde información básica como el nombre y la dirección, hasta datos más sensibles como las preferencias de consumo, la ubicación en tiempo real y los hábitos personales.

El **gran volumen de datos** genera un escenario en el que no siempre es posible garantizar su protección efectiva, especialmente cuando estos datos se transfieren entre países con diferentes normativas sobre privacidad. En este sentido, la **globalización digital** de los servicios de internet y la falta de un consenso internacional sobre las normas de privacidad dificultan la creación de un marco legal uniforme.

Otro desafío importante es la **falta de transparencia** en la manera en que las empresas recopilan, usan y comparten los datos personales. Muchas veces, los usuarios aceptan términos y condiciones sin comprender realmente las implicancias de la recopilación de sus datos, lo que compromete su derecho a la intimidad. A esto se suma el hecho de que muchas veces los sistemas legales nacionales no cuentan con mecanismos adecuados para hacer frente a empresas globales que operan sin someterse a las normativas locales.

El **acceso no autorizado a la información** por parte de actores malintencionados, como hackers, o incluso la vigilancia estatal, constituye otro reto crucial en la protección de la intimidad. A medida que aumenta la interconexión de dispositivos a través del internet de las cosas (IoT), la posibilidad de que la información personal sea comprometida también crece exponencialmente.

Además, la **falta de educación digital** en las personas sobre el manejo de sus datos personales y la importancia de la protección de la intimidad en el entorno digital contribuye a que muchos individuos no sean conscientes de los riesgos que enfrentan al interactuar con plataformas online.

La protección del derecho a la intimidad en la era digital es un desafío complejo que requiere una respuesta jurídica integral y adaptativa. Si bien existen marcos legales internacionales y nacionales que buscan garantizar este derecho, la evolución rápida de la tecnología y el uso generalizado de internet presentan constantes riesgos para la privacidad de las personas. Por ello, es crucial fortalecer las normativas existentes,

fomentar la educación digital y trabajar hacia un equilibrio entre los avances tecnológicos y la protección de los derechos fundamentales.

1.4. Injusto penal y sistemas informáticos

La evolución tecnológica ha tenido un impacto significativo en el ámbito del derecho penal, especialmente en lo que respecta a la protección de los derechos fundamentales, como la intimidad, frente al uso de sistemas informáticos. En la actualidad, los delitos cibernéticos y el manejo indebido de datos personales son temas de creciente preocupación en los sistemas legales, ya que las tecnologías han facilitado la comisión de delitos que anteriormente no existían o que no se podían llevar a cabo con tanta facilidad. Además, el uso de sistemas informáticos en los juzgados ha traído consigo nuevos retos en cuanto a la protección de la intimidad y la garantía de procesos judiciales justos. Este capítulo explora los aspectos más relevantes sobre cómo los sistemas informáticos inciden en el injusto penal, abordando el uso indebido de datos personales, los delitos cibernéticos y el rol de la tecnología en los tribunales.

No existe un único consenso doctrinal sobre el "derecho penal", porque la definición de Injusto penal de Sistemas y Datos Informáticos no es sencilla, y los delitos informáticos engloban todas aquellas conductas que son difíciles de reducir o resumir en una única definición. Por lo tanto, no hay eruditos y tratados doctrinales, por ejemplo:

Villavicencio (2014) lo define como *"un acto dirigido a burlar un sistema de seguridad, es decir, a irrumpir en un ordenador, correo electrónico o sistema de datos utilizando una clave de acceso, acto que típicamente no puede llevarse a cabo sin la ayuda de la tecnología".*

En cuanto a la definición y concepto de delito informático. Acurio (2012), docente de la materia referente al injusto penal de sistemas informáticos de la PUCE, define el delito informático como todo acto o conducta ilícita o ilegal que pueda considerarse delito, y que se comete con la intención de poner en peligro o dañar bienes lícitos, por medio de un sistema informático o sus componentes, con la intención de alterarlo, destruirlo o perturbarlo.

El Dr. Blossiers (2003) señala que el delito informático es un delito instrumental que utiliza un ordenador y que *"el delito informático, aunque actualmente está contemplado en nuestro derecho penal sustantivo, es todavía muy limitado y requiere un derecho penal especial capaz de abarcar una amplia gama de delitos que deben ser complementados",* concluye.

Del mismo modo, el profesor Sáez (2002) señala que "para la mayoría de las doctrinas, no existe la ciberdelincuencia en general, solo un contexto delictuoso complicado asociado a las actuales tecnologías de datos que no puede reducirse a una Única forma jurídica.

Por otro lado, Reyna (2002) señala que la ciberdelincuencia y la delincuencia informática son claramente distintas, pero ambas forman parte del mismo fenómeno delictivo, cuyo nombre real es ciberdelincuencia, que significa delitos que implican el uso de ordenadores o de información en sistemas informáticos.

Asimismo, Blossiers y Calderón (2000) señalan que "están surgiendo en el campo nuevos valores jurídicos colectivos que trascienden al individuo, lo que naturalmente fomenta una mayor intervención del Estado, enriqueciéndolo y fortaleciéndolo al crear nuevos valores de protección que de otra manera quedarían impunes".

El juez Bramont (1997), en su libro El Delito Informático en el Código Penal, sostiene que "el delito informático puede definirse muy ampliamente como un delito en el que se utiliza un sistema de tratamiento o transmisión automática de datos para cometer un delito" y que "la informática El delito no implica de hecho medios legalmente protegidos", señala. No es más que una forma o método de delinquir contra el honor que se encuentra tutelado en la ley penal.

Téllez (1991) lo define como "un acto ilícito en el que se utiliza el ordenador como herramienta u objetivo (concepto atípico) o un acto típico, ilícito o reprobable en el que se utiliza el ordenador como herramienta u objetivo (concepto típico)", e igualmente Sarzana lo define como "un delito en el que se utiliza el ordenador como elemento material o simbólico delito en el que se utiliza el ordenador como forma material o simbólica".

1.4.1. Uso indebido de datos personales en procesos legales

El uso indebido de datos personales en procesos legales representa una de las principales amenazas al derecho a la intimidad en la era digital. Con la digitalización de documentos y la integración de tecnologías en los procedimientos judiciales, se han creado nuevas posibilidades para la recolección, almacenamiento y difusión de información personal de los individuos involucrados en un caso. Aunque los sistemas informáticos pueden mejorar la eficiencia de los procesos judiciales, su mal manejo puede tener consecuencias graves para la privacidad y la seguridad de las personas.

Uno de los principales problemas que surge es la **recopilación masiva de datos** sin el consentimiento explícito de los individuos. En muchos casos, los tribunales y las instituciones legales procesan información sensible de los involucrados en un juicio, como antecedentes penales, datos médicos o detalles personales que, si no son gestionados adecuadamente, pueden ser expuestos a personas no autorizadas. El uso indebido de estos datos puede dar lugar a **vulneraciones de derechos fundamentales**, como la difusión no autorizada de información personal o el uso de estos datos para fines distintos a los originalmente establecidos en el proceso judicial.

Además, la **falta de protocolos de seguridad** en los sistemas informáticos utilizados en los tribunales aumenta el riesgo de que los datos sean **hackeados o manipulados**, lo que no solo afecta la privacidad de los implicados, sino que también pone en peligro la integridad del proceso judicial. La introducción de estos riesgos en un sistema que debería ser imparcial y transparente puede poner en duda la legitimidad de los fallos judiciales y generar desconfianza en la ciudadanía hacia el sistema judicial.

1.4.2. Delitos cibernéticos y su repercusión en la intimidad

Los delitos cibernéticos han proliferado en la última década, y su impacto en la intimidad de las personas es cada vez más significativo. Estos delitos incluyen desde el robo de datos personales, el fraude electrónico, hasta los ataques de **phishing** y el **hacking**, en los cuales los ciberdelincuentes obtienen acceso no autorizado a sistemas informáticos para robar información personal sensible, como contraseñas, datos bancarios, o detalles privados de los individuos.

Una de las repercusiones más graves de los delitos cibernéticos es el **robo de identidad**, donde los delincuentes utilizan los datos obtenidos de manera ilegal para suplantar la identidad de una persona, lo que puede afectar profundamente su vida personal, financiera y profesional. La **violación de la intimidad** en este contexto se manifiesta en la exposición de información personal sin el consentimiento de la persona afectada, lo que puede resultar en la **difusión pública de datos privados**, como fotos, conversaciones privadas, o información confidencial.

El **ciberacoso** es otro fenómeno creciente, donde las tecnologías son utilizadas para hostigar, intimidar o humillar a las personas a través de medios digitales. Este tipo de delito cibernético afecta directamente el derecho a la intimidad, ya que el agresor puede acceder a información privada de las víctimas a través de sus perfiles en redes sociales, correos electrónicos o dispositivos hackeados, provocando un impacto negativo en su bienestar emocional y psicológico.

Por otro lado, el uso de **malware** y otros tipos de software dañino para infiltrarse en los dispositivos personales de los individuos también representa una amenaza grave para la intimidad. Los ciberdelincuentes pueden acceder a fotos, mensajes, grabaciones de audio y video, e incluso controlar remotamente cámaras o micrófonos, lo que compromete la privacidad de la persona afectada de manera irreversible.

1.4.3. Rol de los sistemas informáticos en los juzgados

Los sistemas informáticos en los juzgados han transformado la manera en que se gestionan los procesos judiciales, proporcionando una mayor eficiencia en la administración de justicia, pero también introduciendo nuevos retos en la protección de la intimidad y la integridad de los procedimientos. En primer lugar, la **digitalización de expedientes judiciales** y la implementación de plataformas electrónicas para presentar demandas o realizar audiencias virtuales han permitido agilizar los trámites judiciales y reducir los costos operativos. Estas herramientas también han permitido a los ciudadanos acceder a la información relacionada con su caso de manera más rápida y sencilla.

Sin embargo, el uso de tecnologías en el ámbito judicial también implica que los sistemas informáticos deben ser altamente seguros para evitar la **intercepción de datos sensibles**. La **protección de la intimidad de las partes involucradas** en un juicio se

vuelve crucial, especialmente cuando se trata de casos que involucran información confidencial, como los relacionados con el derecho penal, la salud, o la familia.

El uso de **inteligencia artificial** y algoritmos predictivos en algunos tribunales para apoyar la toma de decisiones o hacer recomendaciones sobre sentencias está generando preocupaciones sobre la imparcialidad del sistema judicial. Si bien estas herramientas pueden mejorar la eficiencia y ayudar a reducir sesgos humanos, su uso en el ámbito penal puede generar cuestionamientos sobre la transparencia y la protección de los derechos de las personas involucradas.

Además, el riesgo de **manipulación de pruebas electrónicas** o de **alteración de registros digitales** es un desafío constante en los juzgados que utilizan tecnología. La capacidad de modificar, borrar o falsificar documentos y evidencias en formato digital puede poner en peligro la integridad de los procesos judiciales y socavar la confianza en el sistema judicial. Por lo tanto, es fundamental que los sistemas informáticos sean sometidos a auditorías regulares y que se implementen protocolos de seguridad rigurosos para evitar la alteración no autorizada de información relevante para el juicio.

La relación entre el derecho penal y los sistemas informáticos plantea una serie de desafíos y oportunidades en la protección de los derechos fundamentales, como la intimidad. El uso indebido de datos personales, los delitos cibernéticos y la implementación de tecnologías en los juzgados tienen un impacto directo en la privacidad de los individuos y en la equidad de los procesos judiciales. Es necesario que los sistemas jurídicos evolucionen junto con las tecnologías, adoptando medidas eficaces de protección de datos y garantizando la transparencia, la imparcialidad y la seguridad en el ámbito judicial.

1.5. La expansión del derecho penal

Dado que el derecho penal es una herramienta particularmente importante para la protección de los bienes jurídicos, es dudoso que su expansión se deba, al menos en parte, a la aparición de un nuevo interés legítimo (un nuevo interés o una nueva apreciación de los intereses existentes). Las razones de esta ampliación de los derechos jurídicos son múltiples, pero aquí nos centraremos en las nuevas realidades en las que viven los individuos, hechos que antes no existían, son poco importantes o inexistentes. Por

ejemplo, las instituciones crediticias y financieras, el declive de las ricas realidades tradicionales y la escasez de bienes, el medio ambiente, los grandes aumentos de valor, los efectos de los cambios sociales y culturales, hay un hecho que siempre ha existido pero que ha sido ignorado y finalmente es un patrimonio histórico y cultural. Necesitamos hacernos las siguientes preguntas. ¿Qué tiene de interesante esta clasificación de la realidad? ¿Vale la pena señalar que hay margen para una extensión razonable del derecho penal? Pero también sorprende mostrar que existen importantes manifestaciones de expansión irracional (Silva, 2006, pp. 11-20).

En tal sentido consideremos como ejemplo, el caso en el que una gran afluencia de dinero criminal en un sector de la economía ha desestabilizado significativamente ese sector, con consecuencias desastrosas. Por lo tanto, es bastante razonable castigar a los responsables de la entrada masiva de dinero negro en el sector financiero como delincuentes contra el sistema económico. Sin embargo, esto no significa que no tenga sentido penalizar todas las transacciones en las que se utilice una cantidad pequeña (incluso moderada) de dinero negro para comprar bienes o pagar servicios. La tipificación del lavado de dinero refleja la relativa expansión del derecho penal (en el caso del lavado de dinero a gran escala) y la expansión desproporcionada de otras formas de lavado de dinero que no se puede decir que afecten de ninguna manera al sistema económico. (Silva, 2006, pág. 11-20).

1.5.1. La importancia del derecho penal en la protección de bienes jurídicos.

Lo interesante de esta clasificación de hechos es la gran, pero desproporcionada, extensión del derecho penal. Detrás de cada evento problemático hay un estereotipo de la sociedad en la que vivimos. Por lo tanto, las nuevas formas de delincuencia difieren porque las formas de delincuencia siempre se ajustan al modelo de la sociedad en la que vivimos. En este sentido, este estudio se centra en nuestra sociedad en la que están surgiendo nuevos riesgos. La sociedad actual se caracteriza por un entorno económico que cambia rápidamente y una innovación tecnológica sin precedentes. Los principales avances tecnológicos han afectado y continúan afectando directamente el bienestar humano. Al mismo tiempo, sus efectos negativos no pueden ser ignorados. Estos incluyen el riesgo humano como fenómeno social estructural (Silva, 2006, pp. 11-20).

Muchos de los riesgos a los que nos enfrentamos provienen de las decisiones de otros ciudadanos en la gestión del desarrollo tecnológico. Son los riesgos más o menos directos a los que se enfrentan las personas (como consumidores, usuarios, usuarios de servicios públicos, etc.) debido a los avances tecnológicos en la industria, la biología, la movilidad, el transporte, la energía nuclear, la informática, las telecomunicaciones, etc. En una sociedad tecnológica cada vez más competitiva, muchos son inmediatamente vistos por otros como una fuente de riesgo personal y financiero y excluidos de él. El ejemplo más claro de esto es el delito cibernético que involucra medios electrónicos e Internet. La relación causal entre la sociedad tecnológica en constante cambio y esta nueva forma de delincuencia es innegable. Además, este nuevo tipo de delincuencia es cometido no solo por individuos, sino también por verdaderas organizaciones criminales que aterrorizan a toda la nación (Silva, 2006, pp. 11-20).

El impacto de estas nuevas tecnologías se presenta como un tema central en el campo de los delitos no intencionales, como los daños causados por "errores tecnológicos", en los que una determinada proporción de accidentes críticos son significativos (p. ej., al conducir un automóvil, en un ascensor). Es inevitable debido a la complejidad de la tecnología. Por lo tanto, es necesario determinar cuándo se produce una “falla técnica”, es decir, si se trata de un riesgo delictivo grave o de un riesgo aceptable y/o permisible (Silva, 2006, p. 46).

Fernández (2012) menciona que las tareas de investigación afloran desde las observaciones en el entorno y no son necesariamente tareas profesionales. En consecuencia, la falta de conocimiento que la investigación trata de comprender es problemática. Hoy en día, el campo de las "tecnologías de la información y la comunicación" se está desarrollando y experimentando importantes cambios. Dado que la información almacenada, procesada y transmitida ilegalmente a través de los sistemas informáticos constituye una infracción de los derechos fundamentales, la Ley Nº 30096, modificada por la Ley Nº 30171, es decir la ley de delitos informáticos, que enmarca el “injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad" (p.11).

1.5.2. Factores que impulsan la ampliación de derechos jurídicos.

En los últimos años, la sociedad ha pasado página y ha desarrollado su modo de vida gracias a los avances del derecho y la tecnología. Hoy en día, el uso de la tecnología se ha convertido en una parte integral de la sociedad y con ella se ha añadido al campo del derecho una nueva jurisprudencia, como el derecho informático.

Los delitos y fraudes informáticos comprenden actos como el fraude, la falsificación, el daño, el engaño, la interferencia y el uso no autorizado de las computadoras y, por lo tanto, se considera necesario promover su regulación y control en la legislación peruana.

Una de las razones del aumento de la ciberdelincuencia es la dificultad de identificación y definir a los autores intelectuales. Como resultado, muchos de estos delitos quedan impunes y la sociedad va perdiendo la fe en un sistema de justicia eficaz, eficiente y oportuna. En este contexto, el Estado ecuatoriano debería reformar la ley ecuatoriana para definir los métodos adecuados de publicidad política y proteger a los infractores, creando así un nuevo tipo de actividad política en Perú.

Con la llegada de la tecnología, la delincuencia ha superado todos los sistemas. La llegada de Internet ha permitido que las formas de cometer estos delitos se globalicen y lleguen a lugares inimaginables de la Tierra. Este comportamiento está creciendo rápidamente y cada día se denuncian más casos que ponen en jaque a la policía y al sistema judicial.

Nuestro país no está exento de esta gran responsabilidad global. Por lo tanto, es importante poner en primer plano este problema con las nuevas actualizaciones y las nuevas estrategias utilizadas por los autores de la ciberdelincuencia. La tecnología de la información ha traído nuevos retos y las profesiones se han adaptado a la era digital. Esto significa que, a nivel mundial, en todos los sectores, todas las profesiones estarán conectadas a la tecnología de la información como signo de interconectividad y, por tanto, utilizarán el acceso a Internet como herramienta para estar en sintonía con las nuevas tecnologías.

Por ello, en nuestro país contamos con la (Unidad Criminalística de Alta Tecnología de la PNP), ocupándose de la investigación de delitos complejos y de la correcta recopilación de pruebas circunstanciales para construir un caso y presentarlo ante fiscales y jueces, una tarea muy importante para los investigadores.

El verdadero problema operativo en este caso es el volumen de datos que hay que analizar, del que el personal de Divindat no es en absoluto responsable. Esto, combinado con el problema de la cooperación entre los operadores de telecomunicaciones y la Policía Nacional de Perú, limita la acción, ya que es un proceso extremadamente lento. Demasiados obstáculos burocráticos.

Por otro lado, está la cooperación internacional, que tampoco es lo suficientemente eficaz y debe mejorarse de inmediato para permitir un verdadero cotejo de la información y la determinación de la situación real en un caso determinado. Esto puede ralentizar el análisis del caso y llevar mucho tiempo para completar el estudio.

Es acá donde entra la participación de la pericia informática forense. Y ahí está el problema, aunque un informe de primera calidad sea elaborado por un forense informático autorizado, cuando el informe se presente al fiscal y, en última instancia, al juez, no se entenderá correctamente, por muy bien traducido que esté, porque tanto el fiscal como el juez carecen de los conocimientos informáticos necesarios para identificar adecuadamente al autor del delito por vía informática. En otras palabras, no todos los problemas son funcionales o técnicos, sino problemas relacionados con el procedimiento, la política, la experiencia, la cooperación, etc., que afectan al proceso de investigación y judicial.

En primer lugar, tenemos que entender que la persona que comete el delito no es sólo un tipo que sale a la calle, al que pillan robando y es identificable, sino que ese delincuente está detrás de una cadena de números, detrás de una red, detrás de un servidor que gestiona activos que se convierten en pruebas. Estos activos son capaces de cambiarse a sí mismos o autodestruirse, están pre programados y se convierten en un activo inestable. En otras palabras, el observador cambia el bien observado. Como en la teoría de Newton, toda acción produce una reacción.

Por lo tanto, nunca se sabe con certeza lo que ocurre en el interior del dispositivo, a menos que se le dé un tratamiento especial. En otras palabras, las pruebas digitales son muy poderosas cuando se recopilan adecuadamente, ya que indican cómo, cuándo y por qué sucedieron los hechos. Pero no basta con hacerlo bien, también hay que manejarlo e interpretarlo correctamente, y ahí es donde entran los jueces y fiscales.

Estamos ante un tipo de abuso que generalmente queda impune porque nuestras autoridades -tanto la judicatura como la policía- no están adecuadamente equipadas y no cuentan con las herramientas y procedimientos adecuados para investigar este tipo de delitos.

Para desarrollar un procedimiento o un método adecuado para investigar los delitos informáticos, es necesario respetar la premisa de que estas prácticas deben ser generalmente aceptadas e implementadas y que se deben seguir procedimientos de persecución penal adecuados en el Perú, ya que este comportamiento social está evolucionando muy rápidamente.

Con respecto a la privacidad, singularmente en el ambiente de las redes sociales, se menciona en la Resolución 73/179 (2018) emitida por la ONU, sobre el derecho a la privacidad en la era digital destaca la necesidad urgente de proteger la privacidad en todos los países y sociedades.

Asimismo, el Reglamento 2016/679 (2018) del Europarlamento, entró en vigor en Europa un 24 de mayo del año 2018; Morales (2018) explica que este reglamento tiene como objetivo garantizar la protección de las personas físicas en relación con el tratamiento de datos personales. En este sentido, el reglamento es un instrumento jurídico aplicable a los operadores de redes.

La preocupación por la protección de este bien fundamental frente a la intromisión de terceros en el entorno virtual no es ajena a la situación de nuestro país, y en este sentido, además de la protección constitucional que ofrecen los artículos 2.6 y 2.7 de la Constitución (1993), se han promulgado diversas leyes para abordar la cuestión, en particular mediante la protección penal. Se han promulgado varias leyes para abordar esta cuestión, especialmente mediante la protección del derecho penal. Así, nuestro Proyecto de Ley 1669-2016, aprobado mediante el Decreto Nº 1410, permite enmendar la sección

154 B del Código Penal vigente a fin de imponer severas penas a quienes distribuyan, hagan circular, etc. imágenes de la vida privada de las personas por ser de carácter sexual.

Estas medidas responden a la urgente necesidad de proteger contra las violaciones de la intimidad y otros derechos derivados del manejo inapropiado del medio social. Una nación con un estado constitucional de derecho, la búsqueda del pleno ejercicio de los derechos fundamentales es primordial, encontrar el equilibrio entre el ejercicio de la libertad de expresión y el ejercicio efectivo del derecho a la intimidad en el marco de las nuevas comunicaciones de masas (WhatsApp, Facebook, MSN Messenger, Twitter, etc.) no es una tarea fácil y debemos ser responsables porque es un legítimo desafío.

Volpato (2016) describe el problema como "una situación en la que el nivel de posibilidades tecnológicas es tan alto que es difícil confiar en la propia tecnología para proporcionar una solución técnica a fin de salvaguardar ciertas legales como la intimidad".

En esta óptica, es que se analizó el menester de aproximarse a esta dificultad, y se abordó el siguiente problema general: ¿Cómo incide el injusto penal de sistemas y datos informáticos en la transgresión del derecho a la intimidad en un Juzgado Unipersonal, 2022? y como problemas específicos se tuvo los siguientes: 1. ¿Cómo incide la dimensión confidencialidad del sistema informático en la transgresión del derecho a la intimidad en un Juzgado Unipersonal, 2022? 2. ¿Cómo incide la dimensión Integridad de datos en la transgresión del derecho a la intimidad en un Juzgado Unipersonal, 2022? 3. ¿Cómo incide la dimensión Integridad de sistemas informáticos en la transgresión del derecho a la intimidad en un Juzgado Unipersonal, 2022? 4. ¿Cuál es el nivel del injusto penal de sistemas y datos informáticos en un juzgado unipersonal, 2022? 5. ¿Cuál es el nivel de la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022?

Respecto a la justificación investigativa, se sostuvo:

Desde una justificación teórica, como afirman Canahuire y Morante (2015), los argumentos teóricos se forman cuando estimulan debates científicos sobre el conocimiento existente, con el objetivo de contrastar teorías, probar resultados y generar epistemologías a partir del conocimiento existente.

Esta investigación genera abstracción y debate sobre las violaciones de los derechos humanos fundamentales, por lo tanto, en el campo del derecho, ya que se presentan teorías, doctrinas, precedentes, leyes nacionales y comparadas, que inevitablemente llevan a la generación de epistemologías existentes.

Asimismo, una justificación practica de acuerdo con Bernal (2006), La investigación puede considerarse justificada desde el punto de vista práctico si su progreso contribuye a la solución de un problema o si no revela tácticas que contribuyan a la solución.

Debido a la ciberdelincuencia que afecta no sólo a los bienes jurídicos sino también a la vida de las personas y las familias, el objetivo es simplificar y comprender mejor los casos.

De manera igual, una Justificación social, la ciudadanía a lo largo de su desarrollo, desde la década de los 70 ha instituido derechos e independencia a libre albedrio calificados como de tercera generación, propios que fueron acreditados por el Estado y promovidos al rango Constitucional, lo que se quiere explorar es sobre la incidencia del Injusto penal de Sistemas y Datos Informáticos en la Transgresión del Derecho a la Intimidad.

Finalmente, el estudio tuvo una justificación metodológica, en este sentido, Bernal (2006) asevera que las observaciones tienen legitimidad metodológica en la investigación si ofrecen nuevos métodos y tácticas para lograr una comprensión válida.

Teniendo en cuenta lo anterior, se definió los siguientes objetivos a alcanzar: objetivo general: Determinar la incidencia del injusto penal de sistemas y datos informáticos en la transgresión del derecho a la intimidad en un Juzgado Unipersonal, 2022 y como objetivo específico 1:Determinar la incidencia de la dimensión confidencialidad del sistema informático en la transgresión del derecho a la intimidad en un Juzgado Unipersonal,2022 y como objetivo específico 2: Determinar la incidencia de la dimensión Integridad de datos en la transgresión del derecho a la intimidad en un Juzgado Unipersonal, 2022 y como objetivo específico 3: Determinar la incidencia de la dimensión Integridad de sistemas informáticos en la transgresión del derecho a la

intimidad n un Juzgado Unipersonal,2022.Objetivo específico 4: Determinar el nivel de la variable injusto penal de sistemas y datos informáticos en un juzgado unipersonal,2022.

Y como último objetivo específico 5: Determinar el nivel de la variable transgresión del derecho a la intimidad en un juzgado penal unipersonal, 2022.

De tal manera que se tuvieron que formular las hipótesis generales que fueron las siguientes:

H1: El Injusto penal de sistemas y datos informáticos incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

H0: El Injusto penal de sistemas y datos informáticos no incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

En relación con las hipótesis específicas, se tuvieron en cuenta a las siguientes:

La dimensión confidencialidad del sistema informático incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

La dimensión Integridad de datos incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

La dimensión Integridad de sistemas informáticos incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

1.6. Antecedentes

Se utilizaron textos internacionales, nacionales y regionales como fuentes académicas que apoyaron el tema de investigación.

El problema en cuestión surgió en la década de 1970 con el desarrollo técnico de las tecnologías de la información y la comunicación, junto con la electrónica y las telecomunicaciones, conocidas como informática. La tecnología de la información es el procesamiento lógico de todos los datos a través de dispositivos y sistemas electrónicos. En este contexto, es importante comprender que los datos en un sistema informático

también se conocen como información, y que obtener datos sin el debido permiso del propietario es una violación de la "privacidad", uno de los derechos básicos a la privacidad. La "Declaración de los Derechos del Hombre y del Ciudadano" (1789) entró en vigor como Constitución integral con el significado de "ley fundamental" en la Constitución de (Weimar, 1919, p. 73).

Así, en el ámbito internacional, tenemos el estudio de doctorado de Volpato (2016) titulado "un enfoque teórico del impacto de las nuevas tecnologías en la privacidad" de la Universidad de Sevilla España, su objetivo es demostrar la necesidad de educar a los ciudadanos en una conciencia renovada de los efectos de estas tecnologías sobre este derecho, concluyendo que "el derecho a la privacidad en la actual sociedad de la información está en crisis, profundizándose y la protección de las tradiciones es cada vez más difícil. Hoy, la mayoría de los ciudadanos desconocen las consecuencias de sus acciones Relacionado con la tecnología de la información, en tal situación, este derecho se torna ficticio" (p. 198).

González (2015), en su investigación de doctorado titulado "los programas de vigilancia a gran escala utilizados por la gobernación en cooperación con el grupo particular transgreden la privacidad "de la Universidad de Castilla de la Mancha, España su objetivo fue analizar la posición legal de los programas de vigilancia a gran escala utilizados por la gobernación en cooperación con el grupo particular transgreden la privacidad, concluyendo "que hoy en día, las personas corren a menudo el riesgo de ver violados sus derechos a la privacidad y a la intimidad por el uso de la tecnología. El alcance del derecho a la privacidad y el derecho a la intimidad está cambiando, y se hizo especial referencia al alcance de los contenidos protegidos por ambos derechos" (p, 230).

Riascos (1999), en su estudio de doctorado sobre "Privacidad, Visión de la Información y Delitos Informáticos" en la Universidad de Lleida, España, afirmó que "En 1981, la Unión Europea adoptó un conjunto de principios relativos al tratamiento electrónico de los datos personales facilitados , como la confidencialidad o el secreto, la confidencialidad del procesamiento los principios de flujo, (a) recolección, (b) almacenamiento, registro y retención, y (c) transmisión, se han establecido en la Directiva .Concluyendo por lo tanto que, "existen reglas claras para la transferencia de datos a nivel nacional o nivel internacional que brinden una protección adecuada contra esto" (p. 154)

Amaya, Ávalos y Jule (2012), en su estudio de derecho de la Universidad de El Salvador, “La Privacidad en la Estructura de la Ley de Intervención Especial en Telecomunicaciones”, su objetivo es identificar los factores limitantes que restringen la relación entre las telecomunicaciones y la privacidad y por tanto exige una adecuada protección estatal, concluyendo que “la protección del derecho fundamental a la intimidad es limitada. Por otro lado, señala que no todos los países cuentan con leyes específicas en materia de telecomunicaciones y aunque las tengan, la ley se limita a casos excepcionales. En cuanto a la jurisprudencia como fuente de derecho, reitera que estas decisiones establecen criterios a tener en cuenta al analizar las invasiones a la intimidad para evitar conflictos con otros derechos” (p. 23).

Guzmán (2013), en su tesis doctoral en jurisprudencia en la Universidad

Complutense de Madrid (España), titulada “El derecho fundamental a la intimidad en México: un análisis bajo la influencia de las normas jurídicas del derecho español”, señala que la asociación es un derecho protegido por el desarrollo de las tecnologías de la comunicación y constituye un derecho propio, aunque siempre asociado a la privacidad, ya que existen múltiples formas de interferir en la información de las personas, concluyendo que “el derecho a la privacidad y a la vida familiar” no otorga a los demás el derecho a entrar en su ámbito personal y familiar y prohíbe el uso y divulgación de tal información”. (p. 156)

Lo mismo ocurre con Zevallos (2013). En su tesis doctoral en derecho en la Universidad Complutense de Madrid (España), "Protección de datos personales: desarrollo del marco legal y sus criterios de aplicación”, su objetivo fue también definir criterios de protección de datos en áreas como las telecomunicaciones, concluyendo “en este contexto, la doctrina de los datos personales, la información, el consentimiento, la finalidad y el tratamiento es un principio general. Concluyendo “que debe ser respetada y ajustada a las medidas que se adopten en su contra, con un abanico de responsabilidades administrativas, civiles y penales si no lo es. respetado el principio de secreto, también conocido como obligación de secreto, que implica la protección de los datos personales de una persona, garantizando así el derecho a controlarlos o revelarlos” (p. 225).

La tesis doctoral de Coronado (2015) de la Universidad Complutense de Madrid (España) pretende contribuir al estudio y debate sobre la libertad de expresión y el

"ciberespacio", una de las cuestiones jurídicas que necesita más regulación. Las principales conclusiones de este informe son, por tanto: Concluyo

"que el ciberespacio es una metaterminología, de la siguiente etimología Convivimos no sólo en el ámbito físico y material, sino también en un ámbito jurídico (la nube) que ahora es de acceso universal, y cuya regulación y respuestas políticas deben ser globales. También afirma que el ciberacoso y el ciberbullying son situaciones con graves consecuencias sociales y que cada vez son más frecuentes debido al impacto de la tecnología en los jóvenes" (p, 213).

Dentro del ámbito nacional, se revisaron los estudios como el de

Espinoza (2018), en su disertación "el derecho a la intimidad no está suficientemente protegido en nuestro país, el Perú" en la Universidad Nacional de San Marcos, su objetivo fue determinar los dispositivos de protección existentes del sistema jurídico peruano, que garantiza el respeto del derecho a la intimidad, concluyendo "Aunque este derecho está ampliamente dispuesto en la norma, incluso a nivel constitucional, no siempre se garantiza de forma efectiva, ya que las personas suelen desconocer el alcance de sus derechos y temen que su violación se haga pública. Esta situación se ve agravada por la falta de protección en este ámbito en la jurisprudencia, es decir, cuando existe un conflicto con el derecho fundamental" (p, 189).

De acuerdo con Gamarra (2015), en su tesis de investigación titulado "Los límites del derecho a la información para garantizar el derecho a la intimidad en

Perú" de la Universidad Jorge Basadre Grohmann de Tacna. Su objetivo principal de su investigación fue determinar los límites del derecho a la información para garantizar el derecho a la intimidad en nuestro país. En concreto, el estudio: Concluyó que la privacidad justifica la limitación del derecho a la información. Esto también implica una restricción de la privacidad. Ambas son características fundamentales e indivisibles del individuo, y ninguna de ellas anula la otra a priori.

En relación a los precedentes en el ámbito local, hallamos a Rojas (2015) en su trabajo de investigación titulado "El régimen normativo que regula el derecho a la intimidad". Su objetivo fue establecer un régimen de libertad de expresión eficaz en el contexto de las nuevas formas de libertad de expresión a través de las nuevas tecnologías, ya que no existe un sistema de vigilancia y control de la información que se transmite en las redes sociales y a través de las plataformas de pseudodenuncia. Su conclusión fue que

la vulneración de este derecho puede ser subsanada mediante la innovación y la reforma, siempre que exista un sistema de protección eficaz que impida la violación de la intimidad basada en el derecho a ejercer la libertad de expresión tal y como está actualmente. Y dentro de las recomendaciones incluyen la modificación de la Constitución para mantener la tipificación de determinados delitos relacionados con el derecho a la intimidad y libertad de expresión.

Es importante señalar aquí que, al examinar las investigaciones anteriores sobre el tema de la investigación, se recurrió principalmente a la investigación internacional y no a los entornos locales, tema que ha sido abordado con menos frecuencia, y en los que la utilidad y la necesidad de la investigación y el desarrollo han estado en conflicto.

Para comenzar con la presentación de las teorías relevantes para el tema de esta investigación, es necesario hablar primero de los derechos fundamentales, ya que Haberle (2003) asegura que "los derechos

constitucionales hacen alusión a un orden de libertad establecido como un factor de habilitación para la transformación continua del orden jurídico que hace posible la acción libre de todas las personas". Es necesario discutir la esencia de estos derechos.

Por lo tanto, los derechos fundamentales de la persona deben ser interpretado como una definición de libertad, como una propiedad inherente al ser humano, que le permite canalizar diversas desavenencias colectivas a través de mecanismos que crean conductas perfectas para la realización de la justicia en situaciones particulares (p. 187).

Asimismo, García (2010) sostiene que "el ser humano es un sujeto que dispone razón, intelecto y es libre. Además, posee deberes y derechos predispuestos por la norma constitucional". Además, como afirma La Torre (2012), "el hombre no es un ser aislado de su ambiente y de su entorno social, por lo cual, como dice el antiguo proverbio romano, "No hay sociedad, sin un ordenamiento jurídico" (p.121).

Así, se desarrolla la opinión de que el derecho cumple un rol en la sociedad y está estrechamente relacionado. Aunado a ello también tiene la función de anexión o vigilancia social, permitiendo la gestión o solución de desacuerdos, permitiendo la organización de la sociedad. Esta función significa, en general, que el derecho trata de controlar el comportamiento de las personas mediante normas jurídicas, utilizando diversos mecanismos como los de protección y represión y los de incentivación y motivación. (La Torre, 2012 p.113).

Díaz (citado en Alarcón, 2007,) interpreta los derechos humanos como

"una condición necesaria para la legitimidad del poder político y del derecho positivo". Desde esta perspectiva, y partiendo de la base de los derechos humanos; estos deben ser tutelados porque es la base del derecho, debemos tratar específicamente la libertad para expresarnos como una característica primordial e inviolable de todo ser humano. Pero no es un derecho absoluto, pues depende, como todos los derechos, de las responsabilidades derivadas dl respeto hacia los demás, en particular el derecho a la intimidad, el respeto al honor, la protección de la vida y la salud y por último a la defensa del bien común (Ivo,2013).

Es interesante destacar los argumentos de autores como Ivo (2013) que explican las grandes diferencias entre los sistemas europeos y norteamericano a la hora de resolver el conflicto de la libertad de opinión y la atribución legitima a la intimidad; digno de mencionar que la libertad de información y de expresión es casi siempre prioritaria en el sistema estadounidense, mientras que en el sistema europeo se da claramente prioridad a la privacidad. Esto se debe a que, en Europa, la opinión liberal predominante son los derechos, que incluye a la intimidad que deriva de la dignidad humana, mientras que, en América del Norte, la opinión predominante es que la libertad de información y de expresión debe tener prioridad si eres una figura pública.

Sin embargo, con relación a la variable 1, Para el derecho a la intimidad, hay que definir el significado de la misma. En este sentido, según García (2011), "la palabra intimidad deriva del latín intimus, indicando el espacio mental reservado de una persona, grupo o familia".

Desde el punto de vista filosófico, la intimidad debe definirse como la capacidad de cada persona de sentir su vida y ser inseparable sin disociarse. Siento mis emociones, las oigo resonar en mí, y a través de ellas siento que estoy vivo y que experimento la vida como la vivo (Martí, 2007).

Asimismo, puede definirse como "el conjunto de aspectos que un individuo quiere guardar sobre sí mismo y su imagen promiscua e intuitiva, excluyendo a los demás de este conocimiento, argumentando que sólo ella lo conoce o que su intervención no afecta a los demás". (López, 2017).

Teorías que aluden a la intimidad:

Según la teoría de Hubmann “esferas o círculos concéntricos”, la intimidad consta de tres esferas, la más amplia se conoce como privacidad e incluye comportamientos, mensajes y expresiones que no queremos que los demás conozcan, la segunda se relaciona con el secreto y la última constituye la intimidad personal (González, 2015).

Martínez (2016), refiriéndose a Pérez Luyo, explica que la intimidad se compone de tres áreas. En primer lugar, el ámbito privado, que se caracteriza por ser más amplio y en el que las personas siguen ejerciendo sus derechos a la intimidad, a la privacidad y a la intimidad personal y familiar, y que, por tanto, debe ser protegido y defendido frente a la persecución de terceros. Y finalmente (la esfera personal), que es la esfera íntima, pero también la esfera pública. Aquí hay aspectos que reflejan la individualidad, como el honor y la imagen personal. Fuera de estos ámbitos están los correspondientes al contexto de la vida pública o social, donde no se puede restringir la participación de terceros.

La teoría del mosaico, en contraste con las teorías anteriores, afirma que lo que es público y lo que es privado es relativo y depende en gran medida de quién sea el individuo del enlace informativo, y que alguna información puede ser irrelevante individualmente pero importante en su conjunto, al igual que las piedrecitas de un mosaico se acumulan para dar una descripción de la persona, y así proporciona la información es valiosa.

Por último, la teoría del "derecho a la intimidad" formulada por William Prosser en la década de 1960 interpreta la intimidad en términos de cuatro aspectos: 1) la intrusión en la intimidad de la vida o los asuntos privados de un individuo; 2) la divulgación de aspectos de la vida o los asuntos privados de un individuo; 3) la divulgación que dañaría la reputación social de un individuo; y 4) la privación del nombre o la persona de un individuo interpretado en términos de aspectos (Porras, 2015).

La privacidad se refiere a la aparición de actividades caracterizadas por realizarse de forma muy privada y sin que sean conocidas por un medio o persona, mientras que se presume que la intimidad se refiere a las actividades que son conocidas públicamente y que se realizan sin infringir los derechos de los demás. En este sentido, la privacidad puede proteger la vida personal, familiar y doméstica de una persona de cualquier evento que implique la difusión o divulgación no autorizada de información sobre ella por parte de un tercero. En este sentido, nadie puede violar la privacidad de otra persona fuera de su consentimiento, y más aún hacer público información sobre ella (Reyes, 2020).

Refiriéndose a Jürgen Habermas, Amaya (2015) describe la privacidad como una condición estrechamente relacionada con la libertad, por un lado, en relación con la intervención de los actores estatales, y por otro lado, como una propiedad que las personas deben controlar, para que esté disponible sólo para lo que y quiénes quieran, dentro de los parámetros que elijan. Esto es lo que afirma el autor. También explica que, para el autor, la esfera privada incluye la familia y las relaciones personales, mientras que la esfera pública está formada por todas las redes de comunicación a través de las cuales nos relacionamos, participamos en la cultura y formamos la opinión pública.

En relación a su procedencia, Martínez (2016) asegura, "aunque este derecho tiene una procedencia estrecha, se reconoce como uno de los derechos y libertades de primera generación, hay discusiones históricas y teóricas, pero no sobre su filosofía y función que cumple dejan claro que es una parte fundamental del concepto civil y político del individuo y de la ciudadanía. Está claro que es una de las libertades".

La Comisión Interamericana (2017) sostiene que este derecho engloba al menos cuatro derechos legítimos: a) el derecho a un espacio protegido de injerencias arbitrarias del Estado o de terceros; b) el derecho a actuar según las propias normas y de acuerdo con el propio proyecto de vida; c) la prohibición de la difusión o distribución de información obtenida sin consentimiento, esto asegurado El derecho a la confidencialidad de los eventos que se desarrollen en este espacio seguro, prohibiendo la difusión o distribución de la información obtenida sin consentimiento.

En el ámbito internacional, el artículo 12 de la DUDH (1948), el artículo 17 del PIDCP (1976), los artículos X y XI de la DUDH del año (1948), el artículo 8 de la CEDAW (1950) y los artículos 11 y 13 de la CDPD (1969) hacen referencia a la protección de este derecho. En el ámbito nacional, los apartados 6 y 7 del artículo 2 de nuestra Constitución (1993) son los primeros que abordan esta cuestión. El artículo 6 protege contra el suministro de información por parte de servicios informáticos públicos y privados que interfiera en la vida privada y familiar, mientras que el artículo 7 protege el honor, la reputación, y la imagen personal.

Asimismo, Ley 29733 (2011), Ley de Protección de Datos, Reglamento DS. 003 2013 JUS (2013). El artículo 1 de la ley tiene por objeto proteger el derecho a la protección de los datos personales y permite su aplicación de conformidad con el artículo 2, inciso 6, de la Constitución y el artículo 2, inciso, que define datos personales como información

relativa a datos personales. Una persona, identificándola o permitiendo identificarla de diversas formas. El apartado del artículo 2 del mismo reglamento define datos personales como cualquier información numérica, alfabética, gráfica, fotográfica, de audio, personal o de otro tipo relacionada con la empresa.

Además, la Ley de Protección del Consumidor de nuestro país (1991) contiene una serie de disposiciones destinadas a proteger este derecho fundamental. Por ejemplo, el capítulo V contiene los delitos típicos relativos a la violación de la intimidad (artículos 154-158), el capítulo III contiene los delitos relativos a la violación de la integridad del domicilio (artículos 159-169) y el capítulo IV contiene los delitos relativos a la transgresión de las comunicaciones clasificadas (artículos 161-164).

En tanto a la segunda variable, Injusto penal de Sistemas y Datos Informáticos, debemos seguir como paradigma a Castells (1996), quien afirma que "vivimos en una situación esquizofrénica en la que las pautas de comunicación social son cada día más tensas". El autor reconoce así que nuestra comunicación es cada día más conflictiva y puede dar lugar a violaciones indiscriminadas de los derechos fundamentales, sobre todo teniendo en cuenta el nuevo entorno virtual en el que nos desarrollamos.

1.7. Regulación de la ciberdelincuencia a nivel internacional

Una serie de organismos gubernamentales han desarrollado una serie de evaluaciones políticas y jurídicas para proteger los derechos derivados de los delitos que surgen del mal uso de la tecnología informática. Esto permite a las partes modificar o incorporar todo lo relacionado con la "ciberdelincuencia" en sus códigos legales.

En este contexto, la OCDE (Organización para la Cooperación y el Desarrollo Económico) introdujo en 1983 el primer derecho penal a nivel internacional para tratar los delitos derivados del mal uso de los sistemas informáticos; en 1986, la OCDE también publicó un informe sobre la ciberdelincuencia, en el que se enumeraban las normas existentes y las reformas propuestas para que las naciones integrantes las siguieran. En 1986 La OCDE, igualmente difundió un dictamen tras la ciberdelincuencia, en el que se enumeran las normas existentes y las reformas propuestas para que las sigan los Estados miembros y se recomienda una lista completa de delitos que los países deberían prohibir y castigar, incluyendo otros delitos a los

que se debería aplicar el derecho penal. Sobre esta base, el Consejo de las Comunidades Europeas decidió respaldar la recomendación sobre la "ciberdelincuencia".

1.7.1. Estructura general del injusto penal de sistemas y datos informáticos

Sujeto activo

En el caso de los delitos informáticos y de datos, el sujeto activo es una persona competente con conocimientos de informática.

Sujeto pasivo

En estos delitos, los datos y los sistemas informáticos también son sujetos pasivos del delito. La información es el contenido de un sistema electrónico que pertenece a una persona natural o jurídica, lo que también la convierte en sujeto pasivo delictivo.

Bien jurídico protegido

En el caso del Injusto penal de Sistemas y Datos Informáticos se debe tener en cuenta que la información, si se almacena, procesa y transmite de forma eficiente, puede dar un provecho sobre la colectividad.

En este sentido, Reyna (2001) destaca que “el derecho a la protección penal como interés económico de la sociedad sería la información que no sólo calificaría como un bien social significativo, sino que también satisfaría la pretensión de ser digna y merecedora de protección”.

Actos delictivos

La Ley 30096 deja claro que el acceso no autorizado a un sistema informático, ya sea por una violación de la seguridad o más allá del nivel autorizado, es ante todo un delito.

1.7.2. Confidencialidad de los sistemas informáticos

Cabe señalar que, dado que la confidencialidad es de suma importancia, para proteger los datos informáticos, sólo deben tener acceso a ellos las personas autorizadas, y una de las formas de romper la confidencialidad es la difusión de información (Bradanovic, 2006).

De igual forma, Ferro (2016) afirma que “la privacidad requiere que solo las agencias, sistemas e individuos autorizados tengan acceso a la información”. Se aplica a toda o parte de la información por medio de un procedimiento de caución conocido como "cifrado". En este contexto, la seguridad informática se entiende como un conjunto de medidas destinadas a restringir la entrada a los datos contenido en un procedimiento electrónico.

Integridad de sistemas informáticos

La integralidad de un programa computarizado significa la seguridad de la información contra la alteración o falsificación, que sólo puede ser alcanzada por personas autorizadas, ya sea en el sector público o privado. (Ferro, 2016).

Del mismo modo, Bradanovic (2006) afirma que "la integralidad es la garantía de que los datos no ha sido invertido, desaparecido, reorganizado, transcrito, etc., ni en el transcurso de emisión o el mecanismo a partir del que se remitió." Lo más importante, la entereza de un sistema informático es un conjunto de medidas destinadas a proteger la autenticidad de los elementos individuales que componen el sistema informático frente a modificaciones que sólo pueden realizar personas autorizadas.

Marco jurídico nacional

- Constitución Política del Perú, 1993.
- Ley 30096 de 2013 - Ley de delitos informáticos.
- Ley 30171 - Por la que se modifica la Ley 30096 de 2014 - "Ley de delitos informáticos".

Derecho comparado

- Colombia "Ley 1273 Ley de protección de información y de los datos", adoptada el 5 de enero de 2009.
- Chile "Ley 19223 Tipifica figuras penales relativas a la Informática" de 1993.
- Código Penal español, modificado por la Ley Orgánica 7/2012 de 2013 y adoptado por la Ley Orgánica 10/1995.
- Código Penal Federal mexicano (1931), revisado y publicado el 25 de enero de 2013.
- Ley especial contra la ciberdelincuencia en Venezuela, 2001.

En cuanto al paradigma en el que se realizó este estudio, cabe aclarar que, de acuerdo con Ramos (2015), al ser este estudio un enfoque cuantitativo, se adoptarán los paradigmas positivistas y pospositivista. También afirma que el positivismo debe entenderse como un paradigma que tiene como objetivo comprobar las hipótesis mediante el uso de métodos estadísticos para identificar las variables que están representadas por valores numéricos. En cuanto al pospositivismo, cree que la realidad puede ser comprendida a partir de leyes estrictas, pero sólo de forma imperfecta, debido a lo incompleto del conocimiento humano y a las limitaciones de los métodos de percepción en este sentido.

CAPÍTULO II

ANÁLISIS DEL ENTORNO DIGITAL

En la actualidad, el entorno digital se ha convertido en un componente esencial de la vida cotidiana y de las actividades sociales, políticas y económicas a nivel global. La transformación digital ha generado un impacto significativo en todos los ámbitos, desde la forma en que nos comunicamos y trabajamos, hasta cómo se gestionan los sistemas judiciales, los negocios, y las instituciones gubernamentales. En este capítulo, se aborda un análisis exhaustivo del entorno digital, centrándose en sus características clave, los retos y oportunidades que presenta, así como su influencia en la evolución de diversas áreas, especialmente en el campo del derecho y la justicia.

El análisis del entorno digital se torna crucial en un contexto en el que la digitalización de procesos y la interconexión global son factores determinantes en la creación de un espacio donde las interacciones, los negocios y los procesos legales se desarrollan cada vez más en plataformas virtuales. El avance de las tecnologías de la información y la comunicación (TIC) ha dado lugar a una expansión de la red global de datos, creando nuevas realidades en las que la información se encuentra más accesible que nunca, pero también más vulnerable a los riesgos de la ciberdelincuencia, la manipulación de datos y la violación de la privacidad.

Este capítulo busca desentrañar cómo el entorno digital influye en el sistema judicial, las prácticas legales y la protección de los derechos fundamentales, con un enfoque particular en el derecho a la intimidad y los desafíos que surgen con la proliferación de nuevas tecnologías. Se explorarán las características del entorno digital actual, desde la infraestructura tecnológica hasta la normativa vigente, y se examinarán los riesgos asociados con la digitalización de los procesos judiciales y su impacto en la equidad y la transparencia de los mismos.

Asimismo, se analizarán las oportunidades que presenta este entorno digital para mejorar la eficiencia y accesibilidad del sistema judicial, además de reflexionar sobre los peligros inherentes a la dependencia de las tecnologías, tales como el acceso no autorizado a datos sensibles, los errores tecnológicos y las amenazas a la integridad del proceso judicial. El capítulo concluirá con una reflexión sobre la necesidad de un marco

regulatorio robusto y actualizado, que permita no solo aprovechar las ventajas de la digitalización, sino también garantizar la protección efectiva de los derechos de los individuos en el contexto digital.

2.1. Avances tecnológicos y su impacto en el sistema judicial

Los avances tecnológicos han transformado profundamente diversos sectores, y el sistema judicial no ha quedado exento de esta evolución. El uso de tecnologías de la información y la comunicación (TIC) en los juzgados ha permitido mejorar la eficiencia en la administración de justicia, facilitar el acceso a la información y promover una mayor transparencia en los procesos legales. Sin embargo, junto con estos beneficios, también han surgido desafíos significativos relacionados con la privacidad, la seguridad y la integridad de los procesos judiciales. Este subcapítulo aborda los principales aspectos de la implementación de tecnologías en los juzgados, así como los beneficios y riesgos asociados con su uso.

2.1.1. Implementación de tecnologías en juzgados

La implementación de tecnologías en los juzgados ha experimentado un avance significativo en las últimas décadas, adaptándose a las necesidades de un sistema judicial moderno y eficiente. A través de la digitalización de procesos y la integración de herramientas tecnológicas, los juzgados han logrado mejorar varios aspectos de su funcionamiento, lo que ha permitido transformar la experiencia de los usuarios y la administración de justicia en general.

Digitalización de expedientes y documentos judiciales: Una de las principales innovaciones tecnológicas en los juzgados ha sido la **digitalización de expedientes judiciales**. Este cambio ha permitido la **eliminación del papeleo físico**, lo que ha reducido considerablemente el espacio de almacenamiento necesario y ha facilitado la consulta de documentos. Los jueces, fiscales, abogados y otros actores del proceso pueden acceder a los documentos judiciales desde cualquier lugar, lo que agiliza el flujo de información y reduce el tiempo necesario para la gestión de los casos. Además, la digitalización de los expedientes contribuye a **reducir el riesgo de pérdida o daño de documentos** debido a factores externos como incendios, inundaciones o accidentes.

Plataformas de gestión judicial y audiencias virtuales: Las plataformas de gestión judicial han permitido la creación de sistemas integrados que centralizan la información sobre los casos, lo que facilita el seguimiento del progreso de los litigios, el cumplimiento de plazos y la asignación de tareas. Estas plataformas suelen incluir funciones para la **presentación electrónica de demandas**, la **notificación automática de resoluciones** y la **gestión de citas y audiencias**.

Las **audiencias virtuales** se han implementado de manera más amplia en muchos países, especialmente tras la pandemia de COVID-19. Estas audiencias han permitido que los procedimientos judiciales se lleven a cabo a distancia, ahorrando tiempo y recursos tanto para las partes involucradas como para el sistema judicial en general. Las audiencias virtuales también han facilitado el acceso a la justicia para personas que viven en áreas remotas o tienen dificultades para asistir físicamente a los tribunales.

Uso de inteligencia artificial (IA) y herramientas de análisis de datos: En algunos sistemas judiciales avanzados, se están utilizando herramientas basadas en **inteligencia artificial (IA)** para **predecir el resultado de casos** o **analizar patrones** en las decisiones judiciales. Estas tecnologías pueden asistir a los jueces y abogados en la toma de decisiones más informadas, basadas en grandes volúmenes de datos. Además, la IA puede mejorar la eficiencia en la clasificación de casos, la identificación de pruebas y la gestión de documentos.

Seguridad de la información y sistemas de protección de datos: La adopción de sistemas informáticos en el ámbito judicial también ha implicado la necesidad de fortalecer las medidas de **seguridad de la información**. Los juzgados deben implementar sistemas de protección de datos y protocolos de ciberseguridad para garantizar la **integridad y confidencialidad** de la información procesada. Esto incluye el uso de **encriptación**, **firewalls** y **accesos restringidos** para proteger tanto los expedientes judiciales como los datos personales de los involucrados.

2.1.2. Beneficios y riesgos del uso de sistemas informáticos

El uso de sistemas informáticos en los juzgados ofrece una serie de beneficios claros, pero también presenta riesgos importantes que deben ser gestionados

adecuadamente para asegurar que la tecnología cumpla con su propósito de mejorar el sistema judicial sin comprometer la privacidad ni la equidad del proceso.

Beneficios:

1. **Mayor eficiencia y rapidez en los procesos judiciales:** El principal beneficio del uso de tecnologías en los juzgados es el aumento de la **eficiencia**. Los sistemas de gestión electrónica permiten un seguimiento más ágil de los casos, reducen el tiempo que los funcionarios deben dedicar al manejo de documentos físicos y facilitan la ejecución de plazos judiciales. Las **audiencias virtuales** también han reducido la duración de los procedimientos y han mejorado la organización de los casos.
2. **Accesibilidad y transparencia:** La digitalización ha mejorado el acceso a la justicia, especialmente para aquellos que no tienen la capacidad de desplazarse fácilmente a los tribunales. Los sistemas judiciales basados en tecnologías digitales también pueden **facilitar la consulta pública de los documentos judiciales**, aumentando la **transparencia** del proceso. Esto permite que los ciudadanos puedan informarse sobre el estado de los casos sin necesidad de hacer largos viajes, lo que mejora la confianza pública en el sistema judicial.
3. **Reducción de costos operativos:** La implementación de tecnologías ha permitido reducir los costos asociados con el manejo de grandes volúmenes de documentos en formato físico. Los costos de almacenamiento, impresión y distribución de documentos han disminuido, lo que genera un ahorro significativo para el sistema judicial y para los contribuyentes.
4. **Mejora en la gestión de recursos y toma de decisiones:** Las herramientas tecnológicas, como la **inteligencia artificial** y los sistemas de gestión, pueden asistir a los jueces y abogados en la **toma de decisiones** mediante el análisis de grandes cantidades de datos. La **automatización de tareas administrativas** también permite a los operadores judiciales centrarse en aspectos más sustantivos de los casos, mejorando así la productividad general del sistema.

Riesgos:

1. **Vulnerabilidad a ciberataques y fraudes electrónicos:**
   El uso de sistemas informáticos en el ámbito judicial aumenta la **vulnerabilidad a ciberataques**. Los datos judiciales, que son extremadamente sensibles, pueden ser objeto de **hackeos**, **robo de información** o manipulación. La pérdida de información clave podría comprometer la integridad del sistema judicial y la confianza pública en su capacidad para administrar justicia de manera imparcial.
2. **Desigualdad en el acceso a la tecnología:**
   A pesar de las ventajas de la digitalización, existe un **riesgo de exclusión** para aquellos que no tienen acceso a las tecnologías necesarias. Esto incluye a personas en áreas rurales, personas con bajos recursos económicos o individuos con discapacidad. El acceso limitado a la tecnología puede crear una **brecha digital** en el acceso a la justicia, lo que afecta negativamente la equidad en el sistema judicial.
3. **Protección de la privacidad y confidencialidad de los datos:**
   La digitalización de los procesos judiciales plantea serias preocupaciones sobre la **protección de la privacidad**. La **confidencialidad** de los documentos y los datos personales de las partes involucradas debe ser rigurosamente garantizada. Si los sistemas de seguridad no son lo suficientemente robustos, los datos pueden ser divulgados de manera inapropiada, comprometiendo el derecho a la intimidad y afectando la confianza en el sistema judicial.
4. **Dependencia de la tecnología y fallos del sistema:**
   Un riesgo adicional es la **dependencia excesiva de la tecnología**. Si los sistemas informáticos fallan o experimentan **problemas técnicos**, pueden interrumpir el curso de los procedimientos judiciales, retrasando casos y afectando la capacidad del sistema para cumplir con los plazos legales. Además, los **errores tecnológicos** pueden comprometer la calidad de las decisiones judiciales si los sistemas de IA utilizados no son lo suficientemente precisos.
5. **Desafíos en la capacitación de los actores judiciales:**
   El uso de nuevas tecnologías requiere que los jueces, fiscales, abogados y otros actores del sistema judicial sean **adecuadamente capacitados** en el uso de estas herramientas. Sin la formación adecuada, los usuarios pueden enfrentar

dificultades para utilizar los sistemas informáticos de manera efectiva, lo que puede ralentizar el proceso judicial y poner en riesgo la calidad del servicio.

La implementación de tecnologías en los juzgados ha revolucionado el sistema judicial, trayendo consigo una serie de **beneficios significativos** en términos de eficiencia, accesibilidad y transparencia. No obstante, estos avances también han generado **nuevos riesgos** relacionados con la seguridad, la privacidad y la equidad. Para aprovechar plenamente las oportunidades que ofrece la tecnología, es crucial implementar medidas de **seguridad adecuadas**, **capacitar a los actores judiciales** y garantizar que la digitalización del sistema judicial no excluya a aquellos que no tienen acceso a la tecnología. La clave estará en encontrar un balance entre los beneficios de la innovación tecnológica y la protección de los derechos fundamentales de los individuos.

2.2. Riesgos asociados al manejo de datos personales

En el vertiginoso contexto de la digitalización global, el manejo de los datos personales se ha convertido en una de las áreas más delicadas, especialmente en sistemas donde la confidencialidad y la integridad son fundamentales. En este capítulo, se profundiza en los riesgos inherentes a la gestión de datos personales en el ámbito judicial, una esfera en la que la protección de la privacidad de los individuos es no solo un requisito ético, sino un mandato legal. Con la creciente dependencia de la tecnología para la gestión de los procesos judiciales, la vulnerabilidad de los sistemas informáticos y la exposición de datos sensibles se han convertido en preocupaciones críticas que afectan tanto a los involucrados en los procedimientos judiciales como al propio funcionamiento del sistema de justicia. El uso inapropiado de datos personales, la exposición no autorizada de información confidencial, y la alteración o pérdida de datos críticos son solo algunos de los riesgos a los que están expuestos los sistemas judiciales modernos.

2.2.1. Brechas de seguridad en sistemas judiciales

Las brechas de seguridad en los sistemas judiciales, entendidas como accesos no autorizados a la información contenida en los sistemas digitales, representan una de las principales amenazas que enfrenta la administración de justicia en la era digital. Estas brechas no solo comprometen la **seguridad informática**, sino que también ponen en

peligro la **confidencialidad** y la **integridad** de los datos judiciales, elementos esenciales en cualquier sistema que pretenda administrar justicia de manera justa, equitativa y conforme al derecho.

Una brecha de seguridad puede ser desencadenada por una **vulnerabilidad técnica** en los sistemas informáticos, una **falla humana** o un **ataque cibernético** por parte de actores externos. En cada uno de estos casos, las consecuencias son graves, ya que el acceso a información privada, confidencial y sensible puede estar a la merced de quienes no tienen la autorización ni el interés de preservar la privacidad de los involucrados. Desde la filtración de pruebas clave en un juicio, hasta la divulgación no autorizada de información personal sensible, las brechas de seguridad ponen en riesgo tanto el bienestar de los individuos como la **confianza pública** en el sistema judicial.

Causas comunes de las brechas de seguridad

Las causas de las brechas de seguridad en los sistemas judiciales son diversas y, a menudo, complejas. Entre las principales se encuentran:

1. **Ciberataques externos:** La ciberdelincuencia es un fenómeno en constante crecimiento, y los sistemas judiciales, debido a la naturaleza de la información que manejan, se han convertido en objetivos atractivos para los **hackers**. Estos atacantes pueden utilizar herramientas como el **phishing**, el **ransomware** o el **malware** para infiltrar los sistemas, obtener acceso no autorizado y robar, cifrar o alterar la información contenida en los expedientes judiciales. Un ataque de ransomware, por ejemplo, puede bloquear el acceso a los datos del sistema hasta que se pague un rescate, dejando a los tribunales paralizados y a los implicados en los casos judiciales en una situación de indefensión.
2. **Errores humanos y fallos operativos:** Aunque los ataques cibernéticos son una amenaza constante, los **errores humanos** siguen siendo una de las causas más comunes de las brechas de seguridad. La falta de entrenamiento adecuado en ciberseguridad para el personal judicial o la gestión inadecuada de contraseñas y accesos pueden generar puntos de vulnerabilidad. En ocasiones, los datos confidenciales pueden ser filtrados por descuidos simples, como el envío de correos electrónicos a destinatarios equivocados o la no implementación de protocolos adecuados de **autenticación de usuarios**.

3. **Accesos internos no autorizados:** La brecha de seguridad no siempre proviene de un ataque externo. Los empleados o contratistas internos que tienen acceso legítimo a los sistemas también pueden **abusar de su posición** para acceder a información sensible sin autorización. Estos accesos no siempre se relacionan con la intención maliciosa de los actores internos, pero en muchos casos, el personal judicial o administrativo podría acceder a datos confidenciales sin las precauciones necesarias, lo que constituye una amenaza considerable.

Impacto de las brechas de seguridad en el sistema judicial

Las consecuencias de una brecha de seguridad en los sistemas judiciales son profundas y van más allá de la pérdida de datos. Las repercusiones más notorias incluyen:

1. **Pérdida de confianza pública:** Las filtraciones de datos pueden erosionar **la confianza pública** en el sistema judicial. La percepción de que el sistema no puede garantizar la protección de los datos sensibles de los ciudadanos puede llevar a la desconfianza generalizada en el proceso judicial, lo que impacta directamente en la legitimidad del mismo. Los ciudadanos deben sentir que sus derechos a la privacidad y a la seguridad están siendo respetados para que confíen en la imparcialidad y equidad de las decisiones judiciales.
2. **Violación de los derechos fundamentales:** El acceso no autorizado o la divulgación indebida de datos personales puede **violar derechos fundamentales** de los individuos, como el derecho a la **privacidad**, el **secreto de las comunicaciones** o incluso el derecho a un **juicio justo**. Los datos personales, como los antecedentes penales, la información médica o la situación financiera, deben ser manejados con extrema cautela, ya que su divulgación no autorizada puede dar lugar a **daños irreparables** tanto para la persona afectada como para la integridad del proceso judicial.
3. **Alteración de la integridad del proceso judicial:** En el ámbito judicial, la **integridad** de los datos y las pruebas es esencial. Las brechas de seguridad pueden llevar a la **alteración de pruebas** cruciales o a la manipulación de la información dentro de los expedientes judiciales. Esto no solo pone en riesgo el **derecho de las partes involucradas** a un proceso judicial justo, sino que

también puede afectar la **veracidad de las decisiones judiciales**, comprometiendo la equidad y la justicia de las sentencias.

2.2.2. Consecuencias legales y éticas de las filtraciones de datos

Las **filtraciones de datos** dentro de los sistemas judiciales no solo tienen implicaciones en términos de seguridad, sino que también traen consigo una serie de **consecuencias legales y éticas** que deben ser cuidadosamente gestionadas. Estas implicaciones se extienden más allá de las instituciones judiciales, afectando a los individuos cuyas vidas se ven invadidas por la exposición no autorizada de su información personal. Es esencial que las organizaciones judiciales cuenten con protocolos claros para abordar las filtraciones de datos y minimizar sus efectos negativos.

Consecuencias legales de las filtraciones de datos

1. **Responsabilidad penal y civil:** En muchas jurisdicciones, las filtraciones de datos judiciales pueden constituir un **delito penal**. Aquellos responsables de la filtración, ya sea por negligencia o malicia, pueden enfrentar **sanciones penales** que van desde **multas** hasta **penas de prisión**. Además, los individuos afectados por la divulgación no autorizada de sus datos pueden demandar a las instituciones responsables por los **daños y perjuicios** sufridos, lo que puede resultar en **compensaciones económicas**.
2. **Violación de la normativa de protección de datos:** Las **leyes de protección de datos**, como el **Reglamento General de Protección de Datos (GDPR)** en Europa, establecen estrictas **obligaciones** sobre cómo se deben manejar y proteger los datos personales. Una filtración de datos en el sistema judicial puede ser una clara violación de estas leyes, lo que puede generar sanciones severas. La **falta de medidas adecuadas de protección** de los datos personales puede resultar en multas millonarias, además de la exigencia de **compensaciones** a las víctimas de la filtración.
3. **Anulación de procesos judiciales:** En el ámbito judicial, si se demuestra que una filtración de datos ha afectado la equidad de un caso, puede llevar a la **anulación de decisiones judiciales** previas o a la repetición de audiencias. La manipulación de pruebas o la divulgación indebida de información puede poner

en entredicho la imparcialidad del proceso, lo que genera la necesidad de revisar o incluso reabrir casos previos, con el consiguiente retraso y costo para todas las partes involucradas.

Consecuencias éticas de las filtraciones de datos

1. **Violación de la confianza profesional:** Los profesionales del ámbito judicial tienen un **deber ético** de proteger la información con la que trabajan. Una filtración de datos compromete este principio fundamental y puede dar lugar a la **pérdida de confianza** tanto de los ciudadanos como de otros actores dentro del sistema judicial. Los **jueces, abogados y demás profesionales** involucrados en el manejo de datos personales deben cumplir con los estándares más altos de **ética profesional** para garantizar que la privacidad de las personas se respete en todo momento.
2. **Daño a la reputación y derechos humanos:** Las filtraciones de datos personales pueden causar **daños irreparables** a la reputación de las personas afectadas. La divulgación no autorizada de información confidencial no solo pone en riesgo la **intimidad** de los individuos, sino que también puede llevar a situaciones de **discriminación**, **persecución** o incluso **violencia física o psicológica**. Estos efectos pueden afectar la dignidad humana y la **integridad** de las personas implicadas, lo que genera una violación ética aún mayor del derecho a la privacidad.
3. **Desconfianza en la justicia:** Las filtraciones de datos generan desconfianza en el sistema judicial, erosionando la **legitimidad** de las decisiones tomadas dentro de él. Los ciudadanos esperan que el sistema judicial garantice su **seguridad** y **confidencialidad**, y cualquier violación de estos principios puede afectar seriamente la percepción pública de la justicia. Esto, a largo plazo, puede socavar la confianza en las instituciones judiciales y disminuir la **participación ciudadana** en los procesos judiciales.

El manejo adecuado de los datos personales en los sistemas judiciales es fundamental para mantener la **confianza pública**, la **seguridad** y la **integridad** del proceso judicial. Las brechas de seguridad y las filtraciones de datos pueden tener consecuencias devastadoras no solo para los individuos afectados, sino también para la

legitimidad del sistema judicial en su conjunto. Por lo tanto, es imprescindible que las instituciones judiciales implementen políticas robustas de **protección de datos** y adopten medidas de **ciberseguridad** para garantizar la protección de la privacidad y la justicia. La responsabilidad recae no solo en los técnicos que gestionan los sistemas, sino también en los profesionales judiciales que deben asegurar que el manejo de la información se haga de acuerdo con los principios más altos de ética y legalidad.

2.3. Brechas normativas en el ámbito digital

En un entorno tan dinámico y en constante cambio como el ámbito digital, uno de los mayores desafíos que enfrentan los sistemas jurídicos es la **adaptación de las leyes** a las nuevas realidades tecnológicas. Las **brechas normativas** en el campo del derecho digital son cada vez más evidentes, especialmente cuando se trata de abordar **delitos digitales** y de establecer regulaciones eficaces para la protección de los **derechos fundamentales** en un mundo cada vez más interconectado. La velocidad con la que evolucionan las tecnologías supera en muchos casos la capacidad de los legisladores para crear marcos normativos que aborden todos los problemas y riesgos emergentes. En este capítulo, se profundiza en las brechas normativas existentes en la legislación relacionada con los delitos digitales y se proponen soluciones para la actualización de las normas que regulan el ciberespacio y las actividades digitales.

2.3.1. Lagunas legislativas en delitos digitales

El concepto de **delito digital** es relativamente nuevo, y, como tal, las leyes que lo abordan no han tenido tiempo suficiente para evolucionar y abarcar todos los aspectos que emergen con la expansión de la **tecnología digital**. Aunque muchos países han promulgado leyes específicas para abordar ciertos tipos de delitos informáticos, como el acceso no autorizado a sistemas, el fraude electrónico o el **ciberacoso**, estas normativas a menudo no abarcan el **complejo panorama digital** actual. En particular, las **lagunas legislativas** se hacen evidentes en varios aspectos clave que limitan la capacidad de los sistemas legales para gestionar adecuadamente los delitos digitales.

1. **Definición y clasificación insuficientes de delitos digitales:** Uno de los principales problemas es la **definición vaga** o **incompleta** de lo que constituye un delito digital en las normativas existentes. Las leyes suelen estar diseñadas

para abordar delitos físicos tradicionales y, por lo tanto, no pueden abarcar toda la gama de **conductas delictivas digitales** que surgen a medida que las tecnologías avanzan. **Delitos como el hackeo**, el **robo de identidad**, el **fraude cibernético** y las **violaciones de privacidad** a través de la recopilación no autorizada de datos personales suelen ser difíciles de encuadrar en las leyes existentes, dado que las legislaciones no siempre capturan adecuadamente las complejidades y la naturaleza del ciberespacio.

2. **Jurisdicción transnacional y delitos globales:** Otro desafío significativo es la **jurisdicción** de las leyes. En muchos casos, los delitos digitales cruzan **fronteras nacionales**, lo que plantea la pregunta de qué jurisdicción se aplica cuando los crímenes ocurren en una red global, como Internet. **Los delitos cibernéticos internacionales** pueden involucrar a actores de diferentes países y pueden ser difíciles de perseguir debido a la falta de acuerdos internacionales o la disparidad en las normativas entre naciones. Esto da lugar a un vacío normativo en cuanto a la cooperación internacional en la lucha contra el crimen digital, dificultando la extradición de los delincuentes cibernéticos y la ejecución de sentencias en los casos transnacionales.
3. **Nuevas formas de delitos digitales:** Las **nuevas tecnologías**, como la **inteligencia artificial**, el **blockchain**, la **realidad aumentada** o el **Internet de las Cosas (IoT)**, están introduciendo nuevas formas de delitos que las legislaciones tradicionales no prevén. **El uso de IA para la creación de deepfakes** (falsificación de videos y audios) o **el aprovechamiento de los sistemas de blockchain para actividades ilícitas** como el lavado de dinero o el tráfico de datos son ejemplos claros de cómo las **leyes actuales** no están preparadas para abordar adecuadamente estas tecnologías emergentes. Las **lagunas normativas** en este sentido dejan a los sistemas judiciales incapaces de castigar estos delitos de manera efectiva.
4. **Protección insuficiente de la privacidad en el ciberespacio:** La **protección de la privacidad** es otro ámbito donde las brechas legislativas son especialmente notorias. La **recolección masiva de datos personales** por parte de las grandes corporaciones digitales y los gobiernos plantea interrogantes sobre cómo **regular la privacidad** en línea, especialmente cuando la legislación de

protección de datos varía enormemente de una jurisdicción a otra. Aunque leyes como el **Reglamento General de Protección de Datos (GDPR)** en Europa han establecido un estándar, muchos países no cuentan con normativas nacionales que proporcionen un marco de protección suficiente. Además, los avances en la **recolección y el análisis de datos personales** a través de tecnologías como el **big data** y la **inteligencia artificial** han dejado obsoletas muchas leyes, pues no contemplan el alcance actual de estas tecnologías ni las posibles amenazas que su uso indebido puede generar.

5. **Impunidad en la ciberdelincuencia:** La **impunidad** en los delitos digitales es otro de los efectos nocivos de las lagunas legislativas. A menudo, los ciberdelincuentes logran operar desde **jurisdicciones donde las leyes no están suficientemente desarrolladas** o son laxa en cuanto a la persecución de delitos informáticos, lo que les permite eludir el castigo. Las sanciones existentes en muchas naciones son insuficientes o no se aplican con la misma rigurosidad que en el ámbito físico. Esto, sumado a la **falta de capacitación especializada** en **ciberseguridad** de los cuerpos policiales y las fuerzas judiciales, contribuye a que los criminales tecnológicos se sientan poco amenazados por el sistema legal.

2.3.2. Propuestas para la actualización normativa

Ante el panorama de **lagunas normativas** en el ámbito digital, es imperativo que los legisladores y las instituciones internacionales trabajen de manera conjunta para **actualizar y adaptar las leyes** a las nuevas realidades digitales. A continuación, se presentan algunas propuestas fundamentales que podrían contribuir a la creación de un marco normativo más robusto, eficaz y adaptable en la lucha contra los delitos digitales:

1. **Revisión y expansión de las definiciones de delitos digitales:** Las leyes deben ser **revisadas** para incorporar de manera clara y precisa una **definición** más amplia de los delitos digitales. Esto incluye la **creación de nuevas categorías** para crímenes cibernéticos específicos, como el uso fraudulento de IA, la **falsificación digital** o la manipulación de **blockchain**. La legislación debe evolucionar para incluir la **protección de nuevos tipos de información** que se gestionan en el entorno digital, desde los **datos personales** hasta las **pruebas electrónicas** utilizadas en los juicios. Este enfoque permitiría que los tribunales

puedan manejar de manera adecuada los casos relacionados con los avances tecnológicos más recientes.

2. **Creación de marcos normativos internacionales para delitos transnacionales:** Es esencial fomentar una **cooperación internacional más estrecha** en la lucha contra los delitos cibernéticos. Esto incluye el desarrollo de acuerdos globales que definan y regulen el crimen digital a nivel transnacional, estableciendo **normativas unificadas** y promoviendo la **cooperación entre países** para la persecución de delincuentes informáticos, independientemente de la jurisdicción en la que se encuentren. Se deben promover acuerdos internacionales para facilitar la **extradición** de ciberdelincuentes y el **intercambio de información** entre agencias de seguridad de diferentes países.
3. **Desarrollo de normativas sobre nuevas tecnologías:** La **inteligencia artificial**, el **blockchain**, y el **Internet de las Cosas** son tecnologías que presentan nuevos retos en términos de regulación. Los legisladores deben trabajar para **anticiparse a los problemas que estas tecnologías pueden generar**, desarrollando normativas específicas que aborden cuestiones como el **uso ético de IA**, el **control de las transacciones digitales** en blockchain, o la **seguridad** en los dispositivos interconectados del IoT. Las leyes deben adaptarse a estos avances para evitar que se conviertan en herramientas utilizadas para la comisión de delitos.
4. **Fortalecimiento de la protección de datos personales:** En la era digital, la protección de los datos personales es una de las cuestiones más críticas. Es necesario que los países adopten leyes más estrictas sobre **privacidad digital** y establezcan **mecanismos de control** más eficaces sobre la recolección, almacenamiento y uso de los datos personales. La **armonización de las leyes de protección de datos** a nivel internacional es esencial, para garantizar que las personas tengan un control claro sobre su información, sin importar la jurisdicción en la que se encuentren. Las empresas y gobiernos deben ser responsables de **proteger estos datos** y de responder ante cualquier filtración o uso indebido.
5. **Capacitación y especialización de los cuerpos judiciales y de seguridad:** Es fundamental que los **agentes judiciales, fiscales y cuerpos de policía** sean

capacitados en los aspectos técnicos de los delitos digitales y en el uso de herramientas especializadas de **ciberseguridad**. La formación continua en tecnologías emergentes y en las normativas de protección de datos es crucial para que los actores del sistema judicial puedan **identificar, procesar y sancionar eficazmente** los delitos informáticos. Esto incluye también la **creación de unidades especializadas** en delitos cibernéticos dentro de las fuerzas de seguridad, con el fin de abordar estos crímenes de forma más eficiente.

Las brechas normativas en el ámbito digital son una realidad que afecta tanto la eficacia de los sistemas judiciales como la protección de los derechos fundamentales de los ciudadanos. La velocidad de los avances tecnológicos exige una respuesta legislativa ágil y dinámica, que sea capaz de abordar los nuevos desafíos que plantea el ciberespacio. Es imperativo que los marcos normativos sean revisados, ampliados y actualizados de forma constante, para asegurar que los delitos digitales sean adecuadamente sancionados y que los derechos de los individuos sean protegidos frente a las nuevas formas de amenaza. Solo a través de una **actualización normativa constante**, acompañada de una mayor **cooperación internacional**, podremos enfrentar los retos del futuro digital con eficacia y justicia.

CAPITULO III

METODOLOGÍA

3.1. Tipo y diseño de investigación

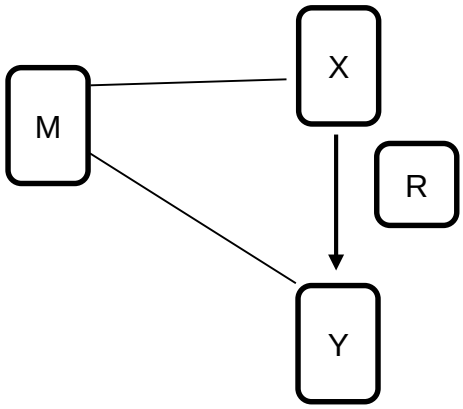
Investigación de tipo fundamental o básica, encaminada a generar conocimiento y teoría a partir del fenómeno estudiado injusto penal de sistemas y datos Informáticos y su incidencia en la transgresión del derecho a la intimidad.

Sobre eso, Beshar (2008) menciona que, "en la investigación básica el objetivo es formular nuevas teorías o modificar las existentes, aumentar los conocimientos científicos o filosóficos, pero no contradecirlos con ningún aspecto práctico" (p.19).). De manera similar, Valderrama (2007) afirma que la investigación básica consiste en descubrir información nueva e interesante, luego tamizarla de manera ordenada y desarrollarla. (pág. 38)

Zorrilla (1993) argumenta que la investigación pura apunta al "avance científico, la mejora del conocimiento teórico, sin preocupación directa por sus posibles aplicaciones o consecuencias prácticas; es más formal y persigue generalizaciones para desarrollar una teoría basada en preceptos" (p. 3).

El estudio corresponde a un diseño **no experimental**, **correlacional causal** y de corte transversal, ya que no se generan situaciones, simplemente se observan situaciones existentes, se recolectan datos en un periodo de tiempo, con el objetivo de conocer la conveniencia a través de las variables de estudio. Asimismo, este estudio utiliza un enfoque cuantitativo porque se consideran medidas numéricas (Relat, 2020).

Su alcance es explicativo, puesto que delinea y especifica cómo incide el injusto penal de sistemas y datos informáticos en la transgresión del derecho a la intimidad (Hernández, et al 2014).



Donde:

M: Profesionales del derecho

X: V1: Injusto penal de sistemas y datos informáticos

Y: V2: Transgresión del Derecho a la Intimidad

R: Relación causal entre injusto penal de sistemas y datos informáticos y transgresión del derecho a la intimidad

3.2. Variables y Operacionalización

De acuerdo con Miranda (2012), una variable de investigación es algo que puede ser medido. La información que se recopilo para responder a nuestras preguntas de investigación son los que nos ayudaron a alcanzar nuestros objetivos.

3.2.1. Variable Independiente (V1): Injusto penal de sistemas y datos informáticos

Comportamiento típico, ilegal y reprobable en el que se utiliza una computadora como herramienta (Núñez, 1996. p. 251-252).

3.2.2. Variable dependiente (V2): Transgresión del derecho a la intimidad.

Se reconocen derechos subjetivos a favor de una persona, para proteger su esfera personal de la injerencia de extraños (Celis 2006. p 7).

3.3. Población, muestra, muestreo y unidad de análisis

3.3.1. Población censal

Según Hurtado (1998), se trata de "un fallo de muestreo en una población pequeña o finita que no afecta a la validez de los resultados" (p. 77). Como la población es pequeña, sólo se puede estudiar la llamada muestra censal. López (1998) considera que "la muestra censal es representativa de toda la población" (p.123).

Mc Guigan (1996) sostiene que "si la población es pequeña, es posible observar a todos los individuos y estudiar a toda la población en lugar de una muestra" (p.158). Tamayo (2003) sugiere llamarla muestra censal porque incluye a todos los trabajadores que participan en la encuesta. Hernández, por su parte, cita a Castro (2003) para afirmar que "si la población es inferior a 50 personas, la población se equipara a la muestra" (p. 69).

Esta investigación tuvo como población censal a 30 profesionales del derecho en un juzgado unipersonal, 2022.

Tabla 1

Profesionales del derecho en un Juzgado Unipersonal, 2022.

Condición	**Sexo**		**Total**	**%**
	Hombres	**Mujeres**		
Juez	8	1	9	30
Relatores	4	0	4	13
Secretarios Judiciales	10	7	17	57
TOTAL	**22**	**8**	**30**	**100**

Criterios de selección de población censal

Criterios de inclusión

1. Profesionales del derecho (Jueces, relatores y secretarios judiciales) en un juzgado unipersonal ,2022.

Criterios de exclusión

1. Profesionales del derecho (Jueces, relatores y secretarios judiciales) que no pertenecen a un juzgado unipersonal, 2022.
2. Profesionales del derecho (Jueces, relatores y secretarios judiciales) no especialistas en materia penal.

Unidad de análisis

Profesionales del derecho en un Juzgado unipersonal, 2022.

3.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

En el presente estudio se eligió como **técnica** la encuesta y como **instrumento** el cuestionario, y su nivel de medición fue a través de una escala ordinal donde sus atributos fueron alto, medio y bajo; con la finalidad de obtener respuestas válidas y fiables que respalden las hipótesis de la investigación, se realizó un análisis de documentos manuales y electrónicos que se presentó en tablas y gráficos (Rojas, 2011) Anexos 3 y 4

Asimismo, se utilizaron también los siguientes instrumentos:

Fichas bibliográficas: Una herramienta para recopilar documentos bibliográficos y cualquier fuente de información relacionada con el Injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad.

Guía de análisis de documental: Una herramienta para recopilar información sobre el Injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad.

Encuesta: los datos se recogieron entrevistando a los participantes para identificar sistemáticamente los conceptos derivados de las preguntas científicas preconcebidas. Esto permitió obtener datos relevantes directamente de los profesionales del derecho para estudiar y fortalecer el sistema legal (Tamayo, 2002).

Cuestionarios: Una herramienta que también incluye preguntas cerradas sobre el Injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad. Una de las principales características de este tipo de herramienta es que las preguntas son cerradas y las respuestas se incluyen en la tabla correspondiente, debido al poco tiempo del que disponen los encuestados para responder a las preguntas. El cuestionario sobre la **variables 1:** Injusto penal de sistemas y datos informáticos cuyo nivel de medición fue: Nivel alto (23 - 30 puntos), nivel medio (15 - 22 puntos) y por ultimo nivel bajo (6 – 14 puntos).Cuyas **dimensiones** fueron 1) La confidencialidad del sistema informático, cuyos indicadores fueron: El acceso deliberado, acceso ilegitimo y la vulneración de seguridad , con 2 ítems cada uno; 2) Integridad de datos, de donde sus indicadores fueron: Dañar, introducir, borrar, deteriorar, alterar, suprimir e inaccesible ,con 1 ítems cada uno; por último 3) Integridad de sistemas informáticos, de lo que sus indicadores fueron: Inutiliza, impedir el acceso, entorpecer su funcionamiento ,con 1 ítems cada uno de ellos y como último indicador de esta dimensión se tuvo a imposibilitar su funcionamiento con (2 ítems).

En el cuestionario sobre la **variable 2 :** Transgresión del Derecho a la intimidad, cuyo nivel de medición fue: Nivel alto (23 - 30 puntos), nivel medio (15 - 22 puntos) y por ultimo nivel bajo (6 – 14 puntos).Así mismo se utilizaron tres **dimensiones:** 1) Intimidad utilizándose como indicadores:

Personal (2 ítems), dignidad (2 ítems), espiritual y cultural con 1 ítems cada uno; 2) La dimensión privacidad con sus respectivos indicadores: Prácticas sexuales (2 ítems), condiciones de salud (1 ítems), comunicaciones personales (2 ítems), y creencias religiosas con 1 solo ítems; en suma se tuvo a 3) Reserva con sus respectivos indicadores: Información (3 ítems),propiedad (1 ítems) y libertad de conciencia con (2 ítems)

3.5. Validez de instrumentos de recolección de datos

Validez de contenido: Los instrumentos utilizados corresponden a los cuestionarios para medir la variable independiente Injusto penal de sistemas y datos

informáticos y la variable dependiente transgresión del derecho a la intimidad; fue realizado por 3 expertos en materia penal Anexo

5.

Validez de criterio: Se aplicó r de Pearson a fin de hallar el coeficiente de correlación entre las variables de estudio.

Confiabilidad de instrumentos de recolección de datos Se obtuvo con la aplicación de los instrumentos a una muestra piloto de 15 abogados especialistas en materia penal de libre desempeño, que reunieron características similares a los integrantes de la población censal, los datos obtenidos se tabularon en una matriz de Excel, estos datos se ingresaron al software SPSS Versión 26, coeficiente de alfa de Cronbach que fue de ,830 para la variable injusto penal y datos informáticos y ,822 para la variable transgresión del derecho a la intimidad. En consecuencia, de la confiabilidad de los cuestionarios de las variables están en un nivel muy aceptable.

3.6. Procedimientos

Una vez establecido los objetivos de estudio e identificado las dimensiones y sus indicadores, provino la identificación y selección de los participantes de acuerdo con los criterios de selección preestablecidos en la población censal.

Para obtener la información necesaria según los sujetos de investigación se utilizó como técnica a la encuesta y para el registro de información un cuestionario de preguntas como instrumento. Asimismo, se ha utilizado la técnica de análisis documental como guía para el análisis de documentos (doctrina), y las fichas bibliográficas para la recopilación de normas nacionales e internacionales (derecho comparado).

A continuación, se informó a los integrantes de la investigación respecto al contenido del estudio, la utilidad de la información proporcionada y los criterios de selección, exhortando su cooperación diligente y voluntariosa.

Luego de aceptada su cooperación, se les notifico acerca de la herramienta de recopilación de información ya validada y su aplicación en el momento y lugar establecido por ellos mismos.

Al término de la recolección de datos, provino el ordenamiento y su clasificación por dimensiones, finalmente se pasó a realizar la triangulación metodológica de la información recopilada de los cuestionarios de preguntas.

En cuanto al análisis de la información recolectada a través de los instrumentos descritos fue ingresada y presentada en el programa estadístico SPSS versión 26. Para la presentación de los resultados se utilizaron tablas de una y doble entrada, de forma numérica y porcentual, finalizando con la triangulación metodológica cuantitativa correspondiente.

3.7. Método de análisis de datos

En el análisis de la información se utilizó métodos aplicados en la jurisprudencia, como son los **métodos de análisis documental**, que a través de la cual se dará a conocer, entender e interpretar cada material, tales como registros, gaceta, textos normativos, y demás fuentes relativas al Injusto penal de sistemas y datos informáticos y transgresión del derecho a la intimidad. **El método conciliación de la información**, sirvió para relacionar datos respecto al Injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad y cotejarlos con otros fundamentos jurídicos o normativa legal. **El Método inductivo**, permitió formar conclusiones desde los datos recolectados de los cuestionarios de preguntas, para luego ser procesados y analizados respectivamente. También se utilizó el **método hermenéutico jurídico**, que se utilizó para estudiar la normativa jurídica de procedimiento.

3.7.1. Estadística descriptiva

Se creó una matriz para marcar las dimensiones de las variables; elaborándose tablas para la distribución de frecuencias y su interpretación en el programa estadístico Excel.

3.7.2. Estadística inferencial

Se utilizó el programa SPPS V 26 para recopilar y procesar información estadística descriptiva y deductiva. Se utilizó la prueba de correlación de Spearman para determinar la correlación de las dimensiones (Confidencialidad de sistema

informático, Integridad de datos, Integridad de sistemas informáticos) de la variable independiente (V1), con la variable dependiente (V2). empleándose r Pearson para el contraste estadístico.

3.8. Aspectos éticos

El estudio de investigación se trabajó acorde a los principios éticos referidos en el Informe Belmont (Polit y Hungler; 2018). El consentimiento informado se extrajo solicitando a los participantes su acorde verbal y escrito para colaborar en la investigación, aclarando su naturaleza, finalidad, las herramientas de recogida de datos, su utilidad y la posibilidad de retirar el consentimiento en cualquier momento.

El principio de beneficencia involucra no menoscabar a los participantes, resguardándolos de detrimentos psicológicos y físicos. Y finalmente, la confidencialidad y el anonimato, a donde no deben exponerse lo reservado de los participantes. Para establecer la fiabilidad de un análisis cuantitativo, se consideró los juicios rígidos de la credibilidad, fiabilidad, conformabilidad y transferibilidad, según Robinson y Tolley (2006). La credibilidad se avaló por medio del valor de la verdad de la confirmación de las respuestas prescritas en los cuestionarios resueltos por los participantes.

La verificabilidad fue comprobada por un asesor que acompaño la secuencia de la investigación desde su inicio hasta el final y complemento con su experticia varias dudas en el transcurso de desarrollo. La validación proporciono a los participantes manifestar con libertad sus vivencias y validar las transcripciones de las mismas mediante su relectura. El estudio igualmente logró asegurar la aplicación a otros entornos manteniendo su esencia investigativa y formativa.

CAPÍTULO IV

ANÁLISIS COMPARATIVO INTERNACIONAL

En un mundo cada vez más globalizado y digitalizado, las cuestiones relacionadas con el derecho digital, la protección de la privacidad y la ciberseguridad han adquirido una dimensión internacional. Las brechas de seguridad, los delitos informáticos y la protección de los derechos fundamentales, como la intimidad, no respetan fronteras geográficas, lo que ha obligado a los países a adaptar sus marcos legislativos a un entorno digital que trasciende las jurisdicciones nacionales. A medida que las tecnologías evolucionan y los delitos digitales se hacen más complejos, los sistemas legales de diversas naciones deben enfrentarse a retos similares, pero cada uno lo hace dentro de sus propios contextos socioculturales, económicos y políticos.

Este capítulo tiene como objetivo realizar un **análisis comparativo internacional** de cómo diferentes países abordan los problemas asociados con el manejo de datos personales, la ciberseguridad y los delitos digitales, con el fin de identificar tanto las **buenas prácticas** como las **brechas** en la legislación global. A través de un análisis detallado de los enfoques normativos adoptados por distintas naciones, se busca ofrecer una visión integral de las **soluciones** y los **desafíos** comunes que enfrentan los sistemas judiciales internacionales ante la creciente digitalización de la sociedad.

La comparación no solo abarcará las legislaciones nacionales en torno a la protección de datos y delitos informáticos, sino que también se examinarán los **acuerdos internacionales** y las **iniciativas transnacionales** que buscan regular de manera coherente las cuestiones cibernéticas a nivel global. En particular, se pondrá énfasis en los esfuerzos para armonizar las políticas de **protección de datos personales**, el **control del cibercrimen** y la **cooperación judicial internacional**. Además, se analizarán los casos emblemáticos de filtraciones de datos y las respuestas de las autoridades internacionales, identificando así las brechas en la protección de la privacidad y la eficacia de las sanciones aplicadas.

Este análisis comparativo proporcionará un contexto más amplio para comprender cómo diferentes países manejan el equilibrio entre la **seguridad nacional**, la **protección de la privacidad** y el **fomento de la innovación tecnológica**. Al mismo tiempo, se discutirán las **mejores prácticas** que podrían adoptarse a nivel global, con el fin de generar un entorno digital más seguro, transparente y justo para los ciudadanos de todas las naciones.

El capítulo concluirá con una reflexión sobre la **necesidad urgente de un marco regulatorio internacional** coherente y robusto que permita abordar las amenazas cibernéticas de manera eficiente, sin sacrificar las libertades individuales ni los derechos fundamentales, adaptándose a las realidades digitales que van cambiando constantemente.

4.1. Casos relevantes en justicia digital y privacidad

La digitalización de los sistemas judiciales ha supuesto grandes avances en términos de eficiencia, accesibilidad y transparencia. Sin embargo, también ha traído consigo desafíos significativos en materia de **protección de la privacidad** y **justicia digital**, especialmente debido a la vulnerabilidad de los datos personales y la creciente amenaza de los delitos cibernéticos. En este capítulo, se realiza un análisis profundo de algunos **casos relevantes** en los cuales la justicia digital y la privacidad han sido puestas a prueba, tanto en **Europa** como en **América Latina**. A través del estudio de estos casos, se buscan extraer lecciones clave sobre cómo las leyes y las políticas de privacidad se implementan en contextos tecnológicos complejos y qué medidas se han tomado para proteger los derechos fundamentales en un entorno digital.

4.1.1. Estudio de casos en Europa

Europa ha sido uno de los continentes pioneros en la creación de normativas y políticas relacionadas con la protección de datos personales y la justicia digital. A través de regulaciones como el **Reglamento General de Protección de Datos (GDPR)**, Europa ha establecido un modelo normativo avanzado para proteger la privacidad de los ciudadanos, mientras intenta equilibrar la necesidad de una **gestión eficiente de la justicia digital**. Sin embargo, a pesar de estos esfuerzos, Europa ha

sido testigo de algunos casos relevantes que han planteado preguntas importantes sobre la efectividad de las leyes existentes y sobre las brechas que aún persisten.

Caso 1: El escándalo de Cambridge Analytica (2018)

Uno de los casos más emblemáticos en Europa relacionado con la **justicia digital** y la **privacidad** fue el escándalo de **Cambridge Analytica**, en el cual se filtraron datos personales de más de 87 millones de usuarios de **Facebook** sin su consentimiento explícito. Aunque el caso no se limitó únicamente a Europa, tuvo un impacto significativo debido a la enorme cantidad de usuarios europeos afectados. En este caso, **Cambridge Analytica** utilizó la información obtenida para influir en elecciones políticas, lo que violó las leyes de protección de datos de varios países, incluidos los miembros de la **Unión Europea (UE)**.

Este caso generó una gran cantidad de interrogantes sobre cómo las plataformas digitales manejan los datos personales de los usuarios y hasta qué punto las políticas de privacidad son eficaces para proteger a los individuos. A nivel europeo, este escándalo evidenció **la necesidad urgente de regulación** en el entorno digital, especialmente en lo que respecta al **consentimiento informado** y al **uso de datos personales con fines comerciales y políticos**.

Respuestas legales y políticas: Como resultado del escándalo, la UE adoptó medidas más estrictas bajo el **GDPR** (Reglamento General de Protección de Datos), el cual otorga a los usuarios un mayor control sobre su información personal, les permite acceder a sus datos, corregirlos, e incluso borrarlos si lo desean. Además, las empresas que infringen las normativas de protección de datos están sujetas a severas sanciones económicas.

El caso Cambridge Analytica subrayó la importancia de la **transparencia en el manejo de datos personales**, la **responsabilidad de las plataformas tecnológicas** y la **necesidad de un marco legal internacional** que proteja la privacidad en la era digital.

Caso 2: El caso Google Spain (2014)

En otro caso importante relacionado con la **justicia digital** y la privacidad, el **Tribunal de Justicia de la Unión Europea (TJUE)** se pronunció en 2014 en el caso **Google Spain SL v. Agencia Española de Protección de Datos**, en el que se abordó el derecho de los ciudadanos a **eliminar información personal de los motores de**

búsqueda. Este caso, conocido como el **derecho al olvido**, surgió cuando un individuo solicitó que se eliminaran los enlaces a noticias antiguas sobre su situación financiera de los resultados de búsqueda de Google.

El TJUE falló a favor del derecho al olvido, estableciendo que los usuarios tienen derecho a **pedir la eliminación de información personal** que ya no sea relevante o que infrinja su derecho a la privacidad, siempre y cuando la información en cuestión no sea de interés público. Este fallo, sin embargo, generó un debate sobre cómo equilibrar el **derecho a la privacidad** con el **derecho a la información**.

Respuestas legales y políticas: El fallo impulsó reformas en las normativas de privacidad de la UE, llevando a una interpretación más amplia del **derecho al olvido** en el contexto digital. También puso de relieve la necesidad de que las plataformas tecnológicas, como Google, tomen un papel activo en la protección de la privacidad, evaluando cuidadosamente las solicitudes de eliminación de datos personales y balanceando estos derechos con los intereses legítimos de acceso a la información pública.

4.1.2. Análisis de experiencias en América Latina

Aunque Europa ha estado a la vanguardia en la regulación de la justicia digital y la privacidad, **América Latina** ha experimentado también avances importantes, aunque con un contexto normativo y político diferente. La región ha adoptado marcos legales para proteger la privacidad, pero las experiencias de varios países muestran que, a pesar de los avances, **persisten brechas significativas** en la implementación de políticas de protección de datos y en la garantía de los derechos digitales de los ciudadanos.

Caso 1: La ley de protección de datos en Brasil (LGPD, 2020)

Brasil, el país más grande de América Latina, promulgó la **Lei Geral de Proteção de Dados Pessoais (LGPD)** en 2020, un paso importante para la protección de la privacidad y la seguridad de los datos personales. La LGPD se inspira en el modelo del **GDPR europeo** y establece **regulaciones sobre el manejo de datos personales** por parte de empresas y gobiernos, así como los derechos de los individuos sobre su información personal.

Este avance se produjo tras una serie de incidentes relacionados con la **filtración de datos personales**, que expusieron la vulnerabilidad de los sistemas de protección de datos en Brasil. La implementación de la LGPD refleja una creciente preocupación por la **privacidad digital** en América Latina, y marca un esfuerzo por adaptarse a las normas internacionales y mejorar la confianza del público en los sistemas digitales.

Desafíos de implementación: A pesar de la promulgación de la LGPD, la implementación efectiva de esta ley enfrenta varios desafíos. El **falta de infraestructura tecnológica** adecuada en muchas regiones, junto con una **deficiente formación en ciberseguridad** de las empresas, dificulta el cumplimiento de la ley. Además, la falta de una **autoridad reguladora fuerte** en algunos países de la región complica la vigilancia y aplicación de las normativas de privacidad.

Caso 2: El escándalo de filtración de datos en México (2019)

México también ha sido escenario de varios casos de filtración de datos, el más notorio ocurrió en 2019, cuando se descubrió que más de 46 millones de registros personales de usuarios de servicios de telefonía móvil y otras plataformas habían sido filtrados. Este caso puso en evidencia las deficiencias en la **protección de datos personales** en el país y la falta de regulación efectiva en torno a la seguridad digital.

El caso resultó en la **inacción gubernamental** por parte de las autoridades competentes, lo que dejó a los usuarios afectados sin una respuesta adecuada a la violación de su privacidad. A pesar de la existencia de la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, las filtraciones revelaron **brechas en la legislación** y en la capacidad del gobierno para hacer cumplir las leyes de protección de datos.

Respuesta y propuestas de reforma: Este incidente subrayó la necesidad de una legislación más robusta en México y en otros países de América Latina, así como de una mayor **cooperación internacional** en el ámbito de la **protección de datos personales**. Los expertos han señalado la importancia de fortalecer **la autoridad reguladora** y **la fiscalización efectiva** de las prácticas comerciales en el manejo de información personal.

Los casos analizados en Europa y América Latina demuestran que, a pesar de los avances significativos en la protección de la **privacidad digital** y la justicia

digital, persisten numerosos desafíos y brechas en la legislación y en la implementación de políticas de protección. En Europa, los casos como Cambridge Analytica y Google Spain muestran la necesidad de **reforzar la regulación** y garantizar el cumplimiento de las leyes existentes. Por otro lado, en América Latina, la promulgación de leyes como la LGPD en Brasil refleja un paso positivo, pero los incidentes de filtración de datos en México y otros países muestran que **la aplicación efectiva de la ley sigue siendo una tarea pendiente**. Es fundamental que tanto los gobiernos como las instituciones judiciales trabajen en conjunto para crear marcos legales robustos y adaptables que no solo respondan a las necesidades tecnológicas actuales, sino que también protejan los derechos fundamentales de los ciudadanos en un entorno digital cada vez más complejo.

4.2. Políticas y buenas prácticas en otros países

A medida que la tecnología sigue avanzando a un ritmo vertiginoso, se hace indispensable que los países ajusten sus marcos regulatorios y las políticas públicas para abordar los nuevos desafíos que plantea el **entorno digital**, especialmente en lo relacionado con la **justicia digital**, la **protección de la privacidad** y la **seguridad de los datos personales**. Las **buenas prácticas** y los **marcos normativos avanzados** de los países que han tomado la iniciativa de adaptar sus sistemas legales y judiciales a las exigencias de la digitalización pueden servir como modelo para otros países que buscan fortalecer sus propios sistemas. Este apartado analiza las **políticas** implementadas por algunos países que han logrado avances significativos en la regulación del entorno digital, especialmente en el contexto judicial, así como la **implementación de sistemas seguros** en los tribunales para garantizar la **protección de datos** y el **debido proceso**.

4.2.1. Marcos normativos avanzados

En muchos países, la **legislación** sobre privacidad y protección de datos ha evolucionado para adaptarse a las nuevas realidades digitales. Algunos de los marcos normativos más avanzados a nivel mundial, como el **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea, han establecido **estándares internacionales** para la protección de la privacidad y el manejo de datos personales.

Sin embargo, otros países también han desarrollado marcos legislativos sólidos que buscan equilibrar la **seguridad**, la **innovación tecnológica** y la **protección de los derechos fundamentales**.

1. El Reglamento General de Protección de Datos (GDPR) de la Unión Europea:

El **GDPR** ha sido una de las legislaciones más avanzadas a nivel mundial en términos de **protección de datos personales**. Adoptado en 2018, el GDPR tiene como objetivo garantizar que **las personas** mantengan el control sobre su información personal, mientras impone a las empresas, gobiernos y otras entidades que manejan estos datos la obligación de ser más **transparentes**, **responsables** y **seguros** con la información que procesan.

Entre sus características más destacadas se encuentran:

- **El derecho al olvido**, que otorga a los individuos el derecho a solicitar la eliminación de sus datos personales en determinadas circunstancias.
- **El principio de minimización de datos**, que establece que solo se debe recolectar la **información mínima necesaria** para cumplir con el propósito específico para el cual se recopilan los datos.
- **El consentimiento explícito**, que exige que las organizaciones obtengan un consentimiento claro y específico de los individuos antes de procesar sus datos.
- **Las multas severas** para aquellos que incumplen las disposiciones del GDPR, lo que ha obligado a muchas empresas a revisar y mejorar sus políticas de privacidad y seguridad.

El GDPR ha sido fundamental en **estandarizar** la protección de datos dentro de la Unión Europea y, al mismo tiempo, ha **influido** en otros países fuera de Europa, que están adoptando normativas similares para alinearse con estos estándares globales.

2. La Ley de Protección de la Privacidad del Consumidor de California (CCPA):

En los Estados Unidos, la **Ley de Protección de la Privacidad del Consumidor de California (CCPA)**, que entró en vigor en 2020, es otro ejemplo de un marco normativo avanzado en el ámbito de la **protección de datos personales**.

Esta ley otorga a los residentes de California el derecho a saber qué datos están siendo recopilados sobre ellos, a solicitar su eliminación y a optar por no permitir que sus datos sean vendidos. A diferencia del GDPR, que es más **estricto y detallado**, el CCPA proporciona un enfoque menos riguroso pero aún así establece **protecciones importantes** en un país donde la legislación sobre privacidad y protección de datos ha sido históricamente fragmentada y débil.

El CCPA ha sido un paso importante para **fortalecer** los derechos de privacidad de los consumidores en los EE. UU., y ha servido de inspiración para otras iniciativas similares en diferentes estados del país.

3. La Ley de Protección de Datos Personales de Brasil (LGPD):

En América Latina, **Brasil** ha dado un paso significativo con la promulgación de la **Lei Geral de Proteção de Dados (LGPD)** en 2020, inspirada en el GDPR europeo. Esta ley establece un marco normativo para la **protección de datos personales** en Brasil y otorga a los ciudadanos una serie de derechos relacionados con sus datos, como el derecho a la **información**, el derecho a la **corrección**, el derecho a la **eliminación de datos** y el derecho a la **portabilidad** de los datos.

Aunque la implementación de la LGPD aún enfrenta desafíos, su adopción representa un avance significativo en la regulación de los datos personales en América Latina y ha puesto a Brasil en el camino hacia un alineamiento con las **normas internacionales de privacidad**.

4. Leyes de ciberseguridad en Singapur y Corea del Sur:

Singapur y Corea del Sur también han sido líderes en el establecimiento de marcos normativos avanzados en el ámbito de la **ciberseguridad**. Ambos países han implementado leyes que regulan el **comercio electrónico**, **la protección de datos personales** y **la protección contra delitos informáticos**, como el **Cibersecurity Act** de Singapur y la **Ley de Seguridad de la Información de Corea del Sur**. Estas legislaciones buscan proteger tanto a los consumidores como a las empresas, estableciendo **requisitos de seguridad** y **responsabilidades** claras para las entidades que operan en el ciberespacio.

4.2.2. Implementación de sistemas seguros en juzgados

Además de los marcos normativos, otro componente esencial para garantizar la **justicia digital** y la **protección de la privacidad** es la implementación de **sistemas seguros** en los juzgados. La digitalización de los procedimientos judiciales implica el uso de plataformas electrónicas para presentar demandas, realizar audiencias y gestionar documentos judiciales. Sin embargo, estas plataformas deben estar **adecuadamente protegidas** para evitar **brechas de seguridad**, **filtraciones de datos** y **manipulaciones** de los expedientes judiciales. A continuación, se describen algunas de las mejores prácticas internacionales para la implementación de sistemas seguros en los tribunales.

1. Plataformas de gestión judicial digital en Estonia:

Estonia es un modelo mundial en términos de **gobierno digital** y ha implementado uno de los sistemas judiciales más avanzados y **seguros** a nivel mundial. El país utiliza plataformas completamente digitalizadas para la gestión de casos, la presentación de pruebas y la realización de audiencias. Uno de los pilares fundamentales de la infraestructura digital en Estonia es el uso de una **identificación electrónica segura** que permite a los ciudadanos interactuar de manera segura con los tribunales y otras instituciones gubernamentales.

Este sistema se basa en una **blockchain pública** que asegura la integridad de los registros judiciales, lo que garantiza que los documentos y las pruebas no puedan ser alterados ni manipulados sin dejar un rastro. Además, el sistema estonio incluye medidas de **cifrado avanzado** y **autenticación multifactorial**, lo que aumenta la seguridad y protege la privacidad de los ciudadanos.

2. Sistema de gestión electrónica de casos en Dinamarca:

Dinamarca también ha implementado un sistema digital avanzado para la **gestión de casos judiciales** que permite a los ciudadanos presentar documentos electrónicamente, recibir notificaciones y acceder a información sobre sus casos de manera online. El sistema utiliza **plataformas encriptadas** que garantizan la **confidencialidad** y **seguridad** de los datos personales involucrados en los procedimientos judiciales.

Además, Dinamarca ha adoptado el principio de **audiencias virtuales** en ciertas circunstancias, lo que no solo mejora la eficiencia del sistema judicial, sino

que también proporciona una **mayor accesibilidad** para personas que no pueden asistir físicamente a los tribunales debido a barreras geográficas o de movilidad.

3. El uso de blockchain en el sistema judicial de Suiza:

Suiza ha explorado el uso de **blockchain** para mejorar la seguridad y la transparencia de los **registros judiciales**. En particular, se han implementado soluciones basadas en blockchain para **autenticar** documentos y contratos judiciales, asegurando que no puedan ser alterados una vez que se han registrado. Esto proporciona una **mayor confianza** en la integridad del proceso judicial y reduce la posibilidad de **fraude** o **manipulación de pruebas**.

El estudio de las **políticas y buenas prácticas** de países con **marcos normativos avanzados** y sistemas judiciales digitalizados nos muestra que la **protección de datos personales** y la **seguridad digital** en el ámbito judicial no son solo un reto, sino también una **oportunidad** para mejorar la transparencia, la eficiencia y el acceso a la justicia. Los ejemplos de **Europa**, **América Latina** y países como **Estonia**, **Dinamarca** y **Suiza** ofrecen modelos valiosos que otros países pueden adaptar y aplicar según sus propias necesidades y contextos. La implementación de **sistemas judiciales seguros**, junto con **marcos normativos sólidos** y **cooperación internacional**, es clave para avanzar hacia un sistema judicial digital más eficiente, seguro y justo para todos.

4.3. Lecciones aprendidas aplicables al contexto local

El análisis de los marcos normativos avanzados, las políticas de privacidad y la implementación de sistemas judiciales seguros en otros países ofrece valiosas **lecciones aprendidas** que pueden ser aplicadas para **fortalecer la privacidad** y mejorar la **adaptación tecnológica** en el contexto local. A medida que los países se esfuerzan por digitalizar sus sistemas judiciales, es crucial que adopten las mejores prácticas internacionales, adaptándolas a sus propias realidades y desafíos. Las experiencias de Europa, América Latina y otras naciones avanzadas pueden servir de guía para diseñar políticas, leyes y estrategias que fortalezcan la protección de los derechos fundamentales en el ámbito judicial, sin comprometer la eficiencia ni el acceso a la justicia.

Este apartado se enfoca en las estrategias para **fortalecer la privacidad en los procesos legales** y las **recomendaciones para la adaptación tecnológica** en el contexto local, basadas en las lecciones derivadas de las experiencias internacionales más destacadas.

4.3.1. Estrategias para fortalecer la privacidad en procesos legales

El **fortalecimiento de la privacidad** en los procesos legales es un componente fundamental para garantizar un **proceso judicial justo** y para proteger los derechos fundamentales de los ciudadanos. En el contexto local, esto requiere no solo el **cumplimiento de normativas internacionales**, sino también la creación de **estrategias adaptadas** a las características sociopolíticas, culturales y económicas del país. A continuación, se exploran algunas de las **estrategias clave** que pueden ser implementadas para mejorar la privacidad en los procesos legales.

1. Implementación de sistemas de autenticación y autorización robustos

Una de las lecciones más claras derivadas de los marcos normativos avanzados, como el **GDPR** europeo, es la necesidad de implementar mecanismos de **autenticación** y **autorización** robustos para el acceso a la información judicial. En muchos sistemas judiciales digitales, el acceso a datos personales y a documentos confidenciales debe ser restringido y monitoreado constantemente para evitar filtraciones no autorizadas.

Recomendaciones:

- **Autenticación multifactorial (MFA):** Implementar sistemas de **autenticación multifactorial** para garantizar que solo las personas autorizadas puedan acceder a la información sensible. Este tipo de autenticación combina algo que el usuario sabe (una contraseña), con algo que tiene (un token o un teléfono móvil) y algo que es (un reconocimiento biométrico), lo que proporciona una capa adicional de seguridad.
- **Control de acceso basado en roles:** Adoptar sistemas de **control de acceso basado en roles (RBAC)**, donde los permisos de acceso sean asignados de acuerdo con el **rol profesional** del usuario dentro del sistema judicial (por ejemplo, juez, abogado, fiscal), garantizando que cada individuo solo tenga acceso a la información necesaria para cumplir con sus funciones.

2. Garantizar la encriptación de datos

La **encriptación** de los datos es otro pilar fundamental en la protección de la privacidad en los procesos legales. La adopción de estándares internacionales de **encriptación** (como **AES-256**) garantiza que, incluso si los datos son interceptados, no puedan ser leídos ni utilizados sin la clave de desencriptación adecuada.

Recomendaciones:

- **Encriptación de extremo a extremo:** Asegurarse de que todos los datos procesados y almacenados en los sistemas judiciales sean encriptados de extremo a extremo, desde el momento en que se ingresan en el sistema hasta que son procesados o presentados ante el tribunal. Esto garantiza que los datos permanezcan seguros, incluso si hay una brecha de seguridad.
- **Encriptación en el tránsito de datos:** Además de encriptar los datos almacenados, es esencial encriptar los **canales de comunicación** entre los usuarios y el sistema judicial, de manera que la información transmitida entre los tribunales y los ciudadanos, abogados o funcionarios judiciales sea completamente segura.

3. Fortalecimiento de la legislación y los derechos de los usuarios

El marco normativo debe ser claramente definido y alineado con los estándares internacionales de **protección de la privacidad** y **protección de datos personales**. Esto incluye el establecimiento de derechos claros para los ciudadanos en relación con la gestión de sus datos, así como las responsabilidades de las entidades judiciales que procesan esa información.

Recomendaciones:

- **Derecho al acceso y rectificación de datos:** Garantizar que los ciudadanos tengan el derecho de **acceder** a la información que los tribunales almacenan sobre ellos, así como de **rectificar** cualquier dato erróneo o desactualizado. Este derecho debe estar claramente establecido en la legislación nacional y ser de fácil ejercicio por parte de los ciudadanos.
- **Derecho al olvido:** Considerar la inclusión de un **derecho al olvido** en las normativas locales, inspirándose en el fallo de la Corte Europea en el caso **Google Spain**. Este derecho permitiría a los ciudadanos solicitar la

eliminación de datos personales obsoletos o irrelevantes para su situación actual.

4. Sensibilización y capacitación en privacidad digital

La capacitación y sensibilización en **protección de datos personales** y **privacidad digital** es esencial para garantizar que los actores judiciales, como jueces, fiscales y abogados, comprendan los riesgos inherentes al manejo de la información digital. Esto incluye la capacitación en las mejores prácticas de seguridad y en el respeto de los derechos fundamentales durante los procedimientos digitales.

Recomendaciones:

- **Programas de formación continua:** Implementar **programas de formación continua** para los actores del sistema judicial, enfocados en la **ciberseguridad**, la **protección de datos personales** y el uso de nuevas tecnologías en el proceso judicial.
- **Sensibilización pública:** Desarrollar campañas de sensibilización dirigidas a la **ciudadanía** sobre la importancia de proteger su **privacidad digital** y cómo pueden ejercer sus derechos en el contexto de los procedimientos judiciales.

4.3.2. Recomendaciones para la adaptación tecnológica

La adaptación tecnológica del sistema judicial local debe ser un proceso estratégico que no solo contemple la **digitalización de los procedimientos**, sino también la **implementación de tecnologías seguras y accesibles** que permitan a los actores judiciales operar con eficacia, mientras protegen los derechos de los ciudadanos. A continuación, se presentan algunas recomendaciones clave basadas en las experiencias internacionales para optimizar la adaptación tecnológica en el contexto local.

1. Integración de tecnologías avanzadas para la gestión de casos judiciales

El uso de **tecnologías avanzadas** en la gestión de los casos judiciales, como **plataformas electrónicas** y **inteligencia artificial (IA)**, puede mejorar significativamente la eficiencia y la transparencia del sistema judicial. Estas herramientas pueden automatizar tareas administrativas, clasificar casos, gestionar audiencias virtuales y predecir resultados basados en patrones históricos.

Recomendaciones:

- **Implementación de inteligencia artificial para predicción de casos:** Desarrollar e implementar herramientas de **IA** que ayuden en la clasificación de casos judiciales, optimizando la asignación de casos y la priorización de los más urgentes. También, las herramientas de IA pueden predecir posibles resultados judiciales basados en patrones previos, ayudando a los jueces y abogados a tomar decisiones informadas.
- **Audiencias virtuales seguras:** Adoptar sistemas seguros para la realización de **audiencias virtuales**, utilizando plataformas que permitan una interacción efectiva entre los jueces, las partes involucradas y los testigos, sin comprometer la **seguridad** de las comunicaciones.

2. Desarrollo de plataformas interoperables entre diversas instituciones

Es esencial que las **plataformas judiciales** sean interoperables no solo dentro del ámbito judicial, sino también con otras instituciones del gobierno, como los registros civiles, las fuerzas de seguridad y las entidades gubernamentales. Esto facilita el intercambio de información entre diversas entidades de manera segura, permitiendo un flujo de trabajo más eficiente y una mayor transparencia.

Recomendaciones:

- **Interoperabilidad entre instituciones gubernamentales:** Crear plataformas digitales que sean **compatibles y seguras** para el intercambio de datos entre diferentes sectores del gobierno. Esto asegurará que toda la información relevante esté disponible cuando sea necesario, sin comprometer la seguridad ni la privacidad.
- **Plataformas unificadas para ciudadanos y profesionales:** Desarrollar un **sistema único** que permita a los ciudadanos presentar documentos judiciales, consultar el estado de su caso, recibir notificaciones y participar en audiencias, todo en un solo portal, asegurando la **accesibilidad** y **usabilidad** del sistema.

3. Inversión en infraestructura tecnológica robusta

Para que la digitalización y la implementación de nuevas tecnologías sean efectivas, es fundamental que los **tribunales** cuenten con una infraestructura tecnológica robusta. Esto incluye **servidores seguros**, **redes de alta velocidad**,

sistemas de almacenamiento en la nube seguros y plataformas de **backup** para prevenir pérdidas de información y **ciberataques**.

Recomendaciones:

- **Inversión en infraestructura de TI:** Asegurar que los tribunales tengan acceso a **infraestructura tecnológica de última generación**, incluyendo sistemas redundantes para el **almacenamiento seguro de datos** y sistemas de recuperación ante desastres. Esto garantiza que los datos judiciales estén protegidos frente a posibles **fallos del sistema** o **ataques cibernéticos**.
- **Protocolos de actualización y mantenimiento de sistemas:** Establecer protocolos regulares de **actualización** y **mantenimiento de software** para garantizar que los sistemas judiciales estén protegidos frente a vulnerabilidades de seguridad y continúen operando con eficiencia.

Las lecciones aprendidas a nivel internacional en relación con la **privacidad digital** y la **adaptación tecnológica** ofrecen un marco valioso para fortalecer el contexto local. A través de estrategias como la **implementación de sistemas seguros** en los juzgados, el **fortalecimiento de la privacidad** en los procesos judiciales y la **adopción de nuevas tecnologías**, se puede construir un sistema judicial digital que sea no solo eficiente, sino también seguro y transparente. La clave radica en integrar las mejores prácticas internacionales con un enfoque que sea adecuado a las realidades locales, garantizando la protección de los derechos fundamentales y el acceso a la justicia para todos los ciudadanos.

CAPÍTULO V

RESULTADOS

En este capítulo se presentan los **resultados** obtenidos a partir del análisis realizado en los capítulos previos, con un enfoque particular en la **evaluación de las políticas**, **prácticas** y **estrategias** que han sido implementadas para garantizar la **seguridad digital**, la **protección de datos personales** y la **justicia digital** en los sistemas judiciales. A través de un enfoque cuantitativo y cualitativo, se exploran los impactos que las normativas internacionales, las buenas prácticas en diversos países y las adaptaciones locales han tenido sobre la **privacidad** de los ciudadanos, la **eficiencia** de los procesos judiciales y la **seguridad** en el manejo de la información.

El objetivo de este capítulo es evaluar, desde una perspectiva comparativa, las **respuestas regulatorias** y la implementación de **tecnologías judiciales** en diferentes contextos y cómo estas han influido en la mejora de la **transparencia**, la **accesibilidad** y la **protección de derechos fundamentales** dentro del ámbito judicial.

Además, se analizan las **lecciones aprendidas** a partir de los estudios de caso presentados en los capítulos anteriores, permitiendo una **reflexión crítica** sobre los avances y desafíos que enfrentan los países al momento de actualizar sus marcos legales y adoptar nuevas tecnologías en el ámbito judicial. Los resultados obtenidos buscan no solo informar sobre las situaciones actuales, sino también ofrecer recomendaciones claras para fortalecer la **infraestructura digital judicial** y mejorar la **protección de datos** en el contexto local.

Este análisis no solo considera los **éxitos alcanzados**, sino también los **obstáculos y brechas** que aún existen, con el fin de ofrecer una visión integral sobre el estado de la justicia digital a nivel global y local, así como las áreas en las que aún se requieren esfuerzos adicionales.

5.1. Estadística descriptiva

Los resultados se analizaron a la luz de los objetivos e hipótesis del estudio. Para la variable 1 se aplicó un cuestionario con 18 ítems y tres dimensiones, cuyo nivel de medición fue: Nivel alto (23 - 30 puntos), nivel medio (15 - 22 puntos) y por último nivel bajo (6 – 14 puntos). Para tabular dicha información se desarrolló los siguientes niveles de calificación.

Tabla 2

Nivel de Injusto penal de Sistemas y Datos Informáticos en un juzgado unipersonal, 2022.

Nivel	Frecuencia	%
Alto	27	90
Medio	3	10
Bajo	00	00
Total	**30**	**100**

Interpretación: Como se observa en la tabla 2, el nivel de la primera variable de estudio (V1) es preponderantemente alto con un 90.0% definido por 27 entrevistados y un 10.0% mostro un nivel medio definido por 3 entrevistados.

Para la segunda variable (V2) se utilizó un cuestionario compuesto por 18 ítems y tres dimensiones, utilizando los mismos criterios de evaluación que para la primera variable. Además, se recogieron datos para las siguientes áreas de evaluación y se presentaron los siguientes niveles de Puntuación.

Tabla 3

Nivel de Transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Nivel	Frecuencia	%
Alto	25	83
Medio	5	17
Bajo	00	00

Total	**30**	**100**

Interpretación: Como se observa en la tabla 3, el nivel de la segunda variable de estudio (V2) es preponderantemente alto con un 83.0% definido por 25 entrevistados y un 17.0% mostro un nivel medio definido por 5 entrevistados.

5.2. Estadística inferencial

5.2.1. Contrastación de hipótesis general

H1: El Injusto penal de sistemas y datos informáticos incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

H0: El Injusto penal de sistemas y datos informáticos no incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Tabla 4

Correlación de las variables injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

			INJUSTO PENAL DE SISTRMAS Y DATOS INFORMATICOS	TRANSGRESION DEL DERECHO A LA INTIMIDAD
Rho de Spearman	INJUSTO PENAL DE SISTEMAS Y DATOS INFORMATICOS	Coeficiente de correlación	1,000	,630**
		Sig. (bilateral)	.	,000
		N	30	30
	TRANSGRESION DEL DERECHO A LA INTIMIDAD	Coeficiente de correlación	,630**	1,000
		Sig. (bilateral)	,000	.
		N	30	30

N = 30
**. Correlación significativa, nivel 0,01 (2 colas).

Interpretación

Tabla 4, se muestra que la relación entre las variables es positiva alta (r = ,630**) porque altas puntuaciones de la variable Injusto penal de sistemas y datos informáticos se corresponde con las altas puntuaciones de la variable transgresión del derecho a la intimidad, por ende, se deduce que existe una incidencia de modo significativa alta.

La verificación de la hipótesis el coeficiente de correlación r de Pearson (tabla 4), arrojó un índice r = ,630**, correspondiendo a una correlación positiva alta y significativa (p = ,000) entre las variables Injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad. Anexo 8

Regresión lineal

Los resultados de la correlación demostraron que el injusto penal de sistemas y datos informáticos incide de modo significativo en la transgresión del derecho a la intimidad en el primer juzgado penal unipersonal de la Libertad, sede Trujillo. El cálculo de la regresión lineal arrojó un r cuadrado = ,700 para la correlación entre la dimensión del injusto penal de sistemas y datos informáticos y la variable transgresión del derecho a la intimidad; esto quiere decir que la variable 1 incide en un 70% en la variable 2, y un 30 % debe ser explicado por otros factores (figura 1)

5.2.2. Contrastación de hipótesis especificas

Hipótesis especifica 1: La dimensión confidencialidad del sistema informático incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Ho: La dimensión confidencialidad del sistema informático no incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Tabla 5

Incidencia de la dimensión confidencialidad del sistema informático en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

			Confidencialidad del sistema informático	Transgresión del derecho a la intimidad
Pearson	Confidencialidad del sistema informático	Coeficiente de correlación	1	,629**
		Sig. (bilateral)		,000
		N	30	30
	Transgresión del derecho a la intimidad	Coeficiente de correlación	,629	1
		Sig. (bilateral)	,000	
		N	30	30

N = 30

**. Correlación significativa, nivel 0,01 (2 colas).

Interpretación

La tabla 5 señala que, según la correlación de Pearson los datos se distribuyen normalmente, concluyendo que existe una relación moderada entre la dimensión confidencialidad del sistema informático y la variable transgresión del derecho a la intimidad (V2) ya que el coeficiente de correlación es de ,629 y existe una sig. (Bilateral) de ,000; deduciéndose una incidencia positiva moderada pero significativa entre la dimensión confidencialidad del sistema informático y la variable transgresión del derecho a la intimidad (V2).Anexo 9

Regresión lineal

Los resultados de la correlación demostraron que la dimensión confidencialidad del sistema informático de la variable 1 incide de modo significativo en la transgresión del derecho a la intimidad en el primer juzgado unipersonal penal de la Libertad, sede Trujillo. El cálculo de la regresión lineal arrojó un r cuadrado = ,039 para la correlación

entre la dimensión confidencialidad del sistema informático de la variable 1 y la transgresión del derecho a la intimidad; en otras palabras, dicha dimensión incidirá en un 39% en la transgresión del derecho a la intimidad y un 61 % debe ser explicado por otros factores.

Hipótesis especifica 2: La dimensión Integridad de datos incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Ho: La dimensión Integridad de datos no incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Tabla 6

Incidencia de la dimensión Integridad de datos en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

			Integridad de datos	Transgresión del derecho a la intimidad
Rho de Spearman	Integridad de datos	Coeficiente de correlación	1,000	,600
		Sig. (bilateral)	.	,000
		N	30	30
	Transgresión del derecho a la intimidad	Coeficiente de correlación	,600	1,000
		Sig.(bilateral)	,000	
		N	30	30

N = 30

**. Correlación significativa, nivel 0,01 (2 colas).

Interpretación

Tabla 6, se señala que acorde a la correlación Rho de Spearman , los datos presentan distribución normal, se concluye que existe una relación positivamente moderada entre la dimensión Integridad de datos y la variable transgresión del derecho a

la intimidad (V2) ya que el coeficiente de correlación fue de ,600 y tiene un sig. (Bilateral) de ,000; deduciéndose una incidencia positivamente moderada pero significativa entre la dimensión Integridad de datos y la variable transgresión del derecho a la intimidad (V2).Anexo 10

Regresión lineal

Los resultados de la correlación demostraron que la dimensión integridad de datos de la variable 1 incide de modo significativo en la transgresión del derecho a la intimidad en el primer juzgado unipersonal penal de la Libertad, sede Trujillo. El cálculo de la regresión lineal arrojó un r cuadrado = ,034 para la correlación entre la dimensión integridad de datos de la variable 1 y la transgresión del derecho a la intimidad; en otras palabras, dicha dimensión incidirá en un 34% en la transgresión del derecho a la intimidad y un 66 % debe ser explicado por otros factores.

Hipótesis especifica 3: La dimensión Integridad de sistemas informáticos incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Ho: La dimensión Integridad de sistemas informáticos no incide de modo significativo en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

Tabla 7

Incidencia de la dimensión Integridad de sistemas informáticos en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022.

	Integridad de sistemas informáticos	Transgresión del derecho a la intimidad

Rho de Spearman	Integridad de sistemas informáticos	Coeficiente de Correlación	1,000	,482
		Sig.(bilateral)		,006
		N	30	30
	Transgresión del derecho a la intimidad	Coeficiente de Correlación	,482	1,000
		Sig.(bilateral)	,006	
		N	30	30

N= 30

**. Correlación significativa, nivel 0,01 (2 colas).

Interpretación

Tabla 7, se señala que acorde a la correlación Rho de Spearman , los datos presentan distribución normal, se concluye que existe una relación positivamente moderada entre la dimensión Integridad de sistemas informáticos y la variable transgresión del derecho a la intimidad (V2) ya que el coeficiente de correlación fue de ,482 y tiene un sig. (Bilateral) de ,006; deduciéndose una incidencia positivamente moderada pero significativa entre la dimensión Integridad de sistemas informáticos y la variable transgresión del derecho a la intimidad (V2).Anexo 11

Regresión lineal

Los resultados de la correlación demostraron que la dimensión integridad de sistemas informáticos de la variable 1 incide de modo significativo en la transgresión del derecho a la intimidad en el primer juzgado unipersonal penal de la Libertad, sede Trujillo. El cálculo de la regresión lineal arrojó un r cuadrado = ,040 para la correlación entre la dimensión integridad de sistemas informáticos de la variable 1 y la transgresión del derecho a la intimidad; en otras palabras, dicha dimensión incidirá en un 40% en la transgresión del derecho a la intimidad y un 60 % debe ser explicado por otros factores.

4.2.2.4 Nivel del injusto penal de sistemas y datos informáticos

Tabla 8

Nivel de Injusto penal de sistemas y datos informáticos en un juzgado unipersonal, 2022.

			TRANSGRESION DEL DERECHO A LA INTIMIDAD		TOTAL
			MEDIO	ALTO	
Injusto penal de sistemas y datos informáticos	MEDIO	Recuento	1	2	3
		Recuento esperado	,3	2,7	3,0
		% del total	3,3	6,6	10,0
	ALTO	Recuento	3	24	27
		Recuento esperado	3,6	24,0	27,0
		% del total	10,0	80,0	90,0
Total		Recuento	3	27	30
		Recuento esperado	3,0	27,0	30,0
		% del total	10,0	90,0	100.00

Interpretación

Como se muestra en la tabla 8 y figura 5 el nivel de la variable Injusto penal de sistemas y datos informáticos (V1), es preponderantemente alto con un 90% establecido por 27 encuestados seguido de un nivel medio 10% establecido por 3 encuestados. Anexo 12

5.2.3. Nivel de la transgresión del derecho a la intimidad

Tabla 9

Nivel de Transgresión del Derecho a la Intimidad en un juzgado unipersonal, 2022.

			TRANSGRESION DEL DERECHO A LA INTIMIDAD		TOTAL
			MEDIO	ALTO	
Injusto penal de sistemas y datos informáticos	MEDIO	Recuento	1	4	5
		Recuento esperado	,3	4,7	5,0
		% del total	3,3	13,3	17,0
	ALTO	Recuento	3	22	25
		Recuento esperado	3,7	23,3	27,0
		% del total	10,0	73,0	83,0
Total		Recuento	5	25	30
		Recuento esperado	5,0	25,0	30,0
		% del total	17,0	83,0	100.00

Interpretación:

Como se muestra en la tabla 9 y figura 6 el nivel de la variable transgresión del derecho a la intimidad (V2), es preponderantemente alto con un 83% establecido por 25 encuestados seguido de un nivel medio con 17% establecido por 5 encuestados.

CAPÍTULO VI

DISCUSIÓN

En este capítulo, se lleva a cabo un análisis reflexivo sobre los **resultados** presentados previamente, con el fin de contextualizarlos dentro del panorama más amplio de la **justicia digital** y la **protección de la privacidad** en los sistemas judiciales. La discusión aborda los principales **hallazgos** y los **desafíos** identificados a lo largo del estudio, proporcionando una interpretación crítica de los **avances tecnológicos**, las **normativas internacionales** y las **buenas prácticas** analizadas, al tiempo que se reflexiona sobre las implicaciones de estos resultados para el contexto local.

A lo largo de este capítulo, se evalúan las **tendencias** observadas en los marcos regulatorios de distintos países, así como las **estrategias implementadas** para mejorar la seguridad digital, proteger los derechos fundamentales y adaptar las tecnologías judiciales a las nuevas exigencias de un mundo digitalizado. Se exploran las **dificultades** encontradas en la aplicación de políticas públicas, la implementación de tecnologías avanzadas y el **cumplimiento de las normativas de privacidad**, resaltando las **brechas existentes** y las áreas que aún requieren atención.

La discusión también pone en evidencia las **lecciones aprendidas** de otros países que han implementado con éxito ciertas estrategias y cómo estas podrían ser **aplicadas** y **ajustadas** al contexto local. Además, se reflexiona sobre la importancia de la **cooperación internacional** en la creación de un entorno digital más seguro y justo, y cómo los **esfuerzos conjuntos** pueden contribuir a superar los desafíos comunes en materia de **ciberseguridad** y **protección de datos personales**.

Finalmente, este capítulo ofrece una **perspectiva crítica** sobre los resultados obtenidos, planteando interrogantes clave sobre el futuro de la **justicia digital** y el **manejo de datos personales** en un mundo cada vez más interconectado, así como sobre el papel que deben jugar los **actores judiciales** y **legisladores** para garantizar la **efectividad** y la **seguridad** de los sistemas judiciales en el ámbito digital.

Considerando la importancia de la regulación del Injusto penal de Sistemas y datos informáticos y la protección de la transgresión del derecho a la intimidad, **el objetivo general** de este estudio fue determinar la incidencia del injusto penal de sistemas y datos

informáticos en la transgresión del derecho a la intimidad. Examinando la hipótesis general, se constató que existe una correlación positiva y significativa (r = ,630**) entre el injusto penal de sistemas y datos informáticos y la transgresión del derecho a la intimidad. Así, el 70% del injusto penal de sistemas y datos informáticos incide de modo significativo en la transgresión del derecho a la intimidad en los profesionales del derecho en un juzgado unipersonal, 2022. El injusto penal de sistemas y datos informáticos, en detalle sus tres dimensiones (la confidencialidad de sistemas informáticos, integridad de datos y la integridad de sistemas informáticos), menoscaban y/o transgreden el derecho a la intimidad, implícita como segunda variable de estudio, en vista de que el tipo penal es pluriofensivo, los profesionales del derecho en un juzgado unipersonal,2022 ;deben tener presente la protección del objeto material (información) contemplado en el uso de las tecnologías de la información (Guerra ,2011 p.106). Todo servidor público debe ser cauteloso en la protección de sus derechos fundamentales como la intimidad y la confidencialidad, entre otros que se encuentran contenidos en los sistemas informáticos (Riascos ,1999 p.89).

Dado que este estudio abarco al injusto penal de sistemas y datos informáticos y sus dimensiones como la confidencialidad de los sistemas informáticos, la integridad de los datos y la integridad de los sistemas informáticos como una nueva forma de delinquir, se identificaron ciertos **objetivos específicos: El primero,** determinar la incidencia de la dimensión confidencialidad del sistema informático en la transgresión del derecho a la intimidad. La prueba de hipótesis confirmo este objetivo al revelar una correlación de modo significativo entre la dimensión confidencialidad de los sistemas informáticos y la segunda variable de estudio (V2); ya que el coeficiente de correlación Pearson fue ,629 existiendo una sig. (Bilateral) de ,000; deduciéndose una incidencia positiva moderada pero significativa entre la dimensión confidencialidad del sistema informático y la variable transgresión del derecho a la intimidad (V2); en otras palabras dicha dimensión incidirá en un 39% en la transgresión del derecho a la intimidad y un 61 % debe ser explicado por otros factores. Estos resultados se relacionan con lo descrito por Amaya y Ávalos (2012), en su estudio sobre la relación entre las telecomunicaciones y el derecho a la intimidad, constataron que las telecomunicaciones limitan la protección del derecho a la intimidad y, en consecuencia, constituyen una infracción si se cometen de forma

ilegal. Además, cualquier intromisión en la intimidad está protegida por el derecho a la intimidad (Guzmán, 2013).

En cuanto al **objetivo específico 2** fue determinar la incidencia de la dimensión Integridad de datos en la transgresión del derecho a la intimidad. La prueba de hipótesis confirmo este objetivo al revelar una correlación de modo significativo entre la dimensión integridad de datos y la segunda variable de estudio (V2); ya que el coeficiente de correlación Pearson fue ,600 existiendo una sig. (Bilateral) de ,000; deduciéndose una incidencia positiva moderada pero significativa entre la dimensión integridad de datos y la variable transgresión del derecho a la intimidad (V2); en otras palabras dicha dimensión incidirá en un 34% en la transgresión del derecho a la intimidad y un 66 % debe ser explicado por otros factores (Zevallos ,2013).

En cuanto al **objetivo específico 3** fue Determinar la incidencia de la dimensión Integridad de sistemas informáticos en la transgresión del derecho a la intimidad. La prueba de hipótesis confirmo este objetivo al revelar una correlación de modo significativo entre la dimensión integridad de sistemas informáticos y la segunda variable de estudio (V2); ya que el coeficiente de correlación Pearson fue ,482 existiendo una sig. (Bilateral) de ,006; deduciéndose una incidencia positiva moderada pero significativa entre la dimensión integridad de datos y la variable transgresión del derecho a la intimidad (V2); en otras palabras dicha dimensión incidirá en un 40% en la transgresión del derecho a la intimidad y un 60 % debe ser explicado por otros factores. “La intimidad es un derecho fundamental que permite a las personas elegir libremente entre distintos ámbitos de su vida, vivir en paz personal, mantener ciertos aspectos de su vida privada y controlar la información personal " (STC No 00009-2014-AI/TC, F.J. 7), y el Estado, como garante de su protección, debe velar por ella.

En cuanto al **objetivo específico 4** fue determinar el nivel de la variable injusto penal de sistemas y datos informáticos. Dicha variable fue la más alta, con un 90%, definido por 27 participantes seguido del nivel medio, con un 10%, definido por 3 participantes.

Esto es consecuente con lo que refiere Acosta (2012) “dice que en su mayoría los Jueces de la Salas Especializadas en materia penal, y otros profesionales de derecho de libre ejercicio; conocen sobre el injusto penal informático y desconocen el procedimiento que hay que seguir en los mismos por no existir la presencia de estas causas en el medio”.

De lo contrario encontramos en el estudio de Morí (2019) donde concluye que los jueces aceptan que existe ausencia y desconocimiento de tecnológica en delitos informáticos, retrasando la labor de los operadores de justicia en la investigación y juzgamiento de estos delitos y la protección penal de la intimidad.

Por último, dentro de los resultados también se tuvo al **quinto objetivo específico** siendo este determinar el nivel de la variable transgresión del derecho a la intimidad. Dicha variable presento un nivel alto, con un 83%, definido por 25 participantes seguido del nivel medio, con un 17%, definido por 5 participantes. Este resultado tiene relación con la sentencia número 05-2009PHD/TC, de fecha 22 de junio de 2010, emitida por el TC donde desarrolla algunos criterios relacionados con el derecho a la intimidad "No cabe duda de que el derecho a la intimidad, protegido por una constitución política, es un concepto jurídico que algunos consideran ambiguo. No obstante, creemos que hay que plantear una cuestión previa al respecto. El concepto de privacidad puede interpretarse desde diferentes ángulos. Algunos consideran que es una parte de la vida de una persona que no es accesible al público y, por lo tanto, no debería ser accesible a nadie. Sin embargo, es mejor tratar de darle un significado positivo. Por lo tanto, es conveniente partir de la premisa de que (entre otras cosas) en la esfera privada cada uno es libre de desarrollar y promover su propia individualidad. Por lo tanto, se trata de información, hechos o circunstancias que no son generalmente conocidos por el público, que son verdaderos, que están destinados únicamente a la persona interesada o a sus allegados, y que causarían un daño cierto si fueran revelados o conocidos por otra persona" (Espinoza, 2018 p. 89).

CONCLUSIONES

En este capítulo, se lleva a cabo un análisis detallado y reflexivo sobre los resultados obtenidos en el estudio, profundizando en cómo las variables del **injusto penal de sistemas y datos informáticos** impactan en la **transgresión del derecho a la intimidad**. A lo largo de esta discusión, se desglosarán las interrelaciones entre estas variables, se analizarán sus implicaciones y se abordarán las posibles explicaciones para los porcentajes de incidencia observados en el estudio. Las conclusiones derivadas de este análisis no solo iluminan la dinámica de la protección de datos en el entorno digital, sino que también ofrecen perspectivas valiosas sobre las **tendencias judiciales** y la **evolución legislativa** en cuanto a la **privacidad digital**.

En primer lugar, los resultados del estudio realizados con los **profesionales del derecho** en el contexto investigado nos han mostrado una **correlación significativa** entre el **injusto penal de sistemas y datos informáticos** y la **transgresión del derecho a la intimidad**. El análisis de las relaciones entre las variables sugiere que las dimensiones de este injusto penal —es decir, la manipulación y el uso indebido de sistemas y datos informáticos— tienen un impacto considerable sobre la **privacidad de los individuos**, afectando el derecho a la intimidad de manera **sustancial**. Según los datos recabados, **el 70% de la incidencia** de la transgresión del derecho a la intimidad puede ser explicado por las acciones relacionadas con el injusto penal en cuestión, mientras que **un 30%** restante está condicionado por factores adicionales, como las características del sistema judicial, la falta de medidas de ciberseguridad o la inadecuada protección de datos.

Primera Dimensión: Confidencialidad del sistema informático

En relación con la primera dimensión, **la confidencialidad del sistema informático**, el estudio muestra que esta variable tiene una **incidencia moderada pero significativa** en la transgresión del derecho a la intimidad. A través de la recopilación de datos, se evidencia que un **39%** de la transgresión del derecho a la intimidad puede ser atribuida directamente a los problemas de confidencialidad en los sistemas informáticos, es decir, el uso inapropiado de información sensible que debería estar protegida. Este resultado señala que, aunque la confidencialidad es un componente esencial en la protección de la privacidad, hay otros factores que contribuyen a la vulnerabilidad de los

datos personales. Un **61%** de la incidencia, por tanto, debe ser explicado por otras variables, como la falta de control sobre el acceso a la información, la filtración de datos, o la implementación insuficiente de medidas de seguridad.

Este hallazgo subraya la importancia de desarrollar políticas y sistemas que garanticen la **protección de la información confidencial** a través de tecnologías como la **encriptación avanzada**, **protocolos de acceso restringido** y **auditorías de seguridad** continuas. Sin una infraestructura adecuada que salvaguarde los datos, los sistemas judiciales continúan siendo vulnerables a la explotación ilícita de la información.

Segunda Dimensión: Integridad de los datos

En cuanto a la segunda dimensión del **injusto penal de sistemas y datos informáticos**, relacionada con la **integridad de los datos**, los resultados muestran que esta también tiene una **incidencia moderada pero significativa** en la transgresión del derecho a la intimidad. **El 34%** de la transgresión de la intimidad se puede atribuir a la alteración o manipulación de datos personales almacenados en los sistemas judiciales. Este porcentaje resalta la relevancia de **mantener la integridad de los datos** dentro del proceso judicial, ya que la alteración no autorizada de los mismos puede comprometer no solo la privacidad de los individuos, sino también la **equidad** y la **transparencia** de las decisiones judiciales.

Este resultado hace patente la necesidad de **reforzar las políticas de seguridad** dentro de las plataformas judiciales, utilizando tecnologías como **blockchain** para garantizar que los registros judiciales y las pruebas electrónicas sean **inalterables** una vez almacenadas. Además, se destaca la importancia de la **auditoría digital** y el **seguimiento en tiempo real** de la integridad de los datos, para detectar de inmediato cualquier intento de alteración o manipulación.

Tercera Dimensión: Integridad de los sistemas informáticos

Finalmente, la tercera dimensión relacionada con la **integridad de los sistemas informáticos** muestra también una **incidencia moderada pero significativa** en la transgresión del derecho a la intimidad. Con un **40%** de la transgresión atribuida a la integridad de los sistemas, los resultados indican que la **vulnerabilidad de los sistemas judiciales** en términos de infraestructura digital representa un factor importante en las

violaciones a la privacidad. Los ataques a la infraestructura tecnológica, como el **hacking** o la **alteración de sistemas judiciales**, pueden exponer datos sensibles y comprometer seriamente la privacidad de los individuos involucrados en los procesos judiciales.

Este resultado pone en evidencia que **fortalecer la infraestructura tecnológica** en los tribunales es crucial para garantizar la **seguridad cibernética**. El uso de **sistemas resistentes a intrusiones** y la implementación de **redes de protección avanzadas** son elementos clave para minimizar el riesgo de brechas de seguridad que podrían comprometer la privacidad de los ciudadanos.

En cuanto a los resultados de los **niveles de transgresión** del derecho a la intimidad en el contexto local, el estudio revela que la mayoría de los **profesionales del derecho** entrevistados perciben un **nivel alto** de incidencia del injusto penal de sistemas y datos informáticos en las violaciones de la intimidad. De hecho, el **90%** de los entrevistados identificó un nivel alto de incidencia, lo que resalta la conciencia generalizada sobre los **riesgos** asociados con la **digitalización** y la **protección de datos** en el ámbito judicial. Solo un pequeño porcentaje (10%) de los entrevistados percibió un nivel medio de incidencia, lo que sugiere que el **consenso sobre la vulnerabilidad** del sistema judicial digital es mayoritario.

Por otro lado, en relación con la **transgresión del derecho a la intimidad**, un **83%** de los entrevistados coincidió en que esta transgresión se da en un **nivel alto**, lo que refleja la preocupación generalizada sobre el impacto de las brechas de seguridad y la manipulación de datos personales dentro del sistema judicial. Esta alta percepción de transgresión es consistente con los resultados obtenidos en los análisis previos, que muestran que la **incidencia del injusto penal** sobre la intimidad es considerablemente alta, afectando en un **83%** a la privacidad de los individuos involucrados en los procesos judiciales.

En general, los resultados sugieren que, si bien existen esfuerzos significativos para mejorar la **seguridad** y la **protección de la privacidad** en los sistemas judiciales, aún persisten **brechas significativas** que requieren atención urgente. La implementación de **tecnologías avanzadas** de protección de datos, la mejora de la **formación en ciberseguridad** y la creación de **marcos normativos más robustos** son fundamentales para mitigar los riesgos asociados con la **violación del derecho a la intimidad** en el contexto judicial. Las estrategias propuestas en el análisis, que incluyen **la mejora de la**

infraestructura tecnológica y el **refuerzo de las políticas de privacidad**, son esenciales para fortalecer la **confianza pública** en el sistema judicial y garantizar un **proceso judicial justo**, equitativo y seguro en la era digital.

Los porcentajes de incidencia observados, combinados con las percepciones de los profesionales del derecho, destacan la urgencia de avanzar en estas áreas y subrayan la necesidad de una **acción inmediata** para cerrar las brechas que todavía existen en los sistemas judiciales locales. Las **recomendaciones y medidas de seguridad** propuestas en este estudio son fundamentales para garantizar que los sistemas judiciales no solo sean eficientes, sino también **seguros**, **transparente** y **respetuosos** de los derechos fundamentales de los individuos.

RECOMENDACIONES

En un entorno contemporáneo donde la **tecnología** juega un papel central en los procesos judiciales y en la gestión de datos, es esencial que los **profesionales del derecho** comprendan profundamente las implicaciones legales y éticas asociadas al uso de tecnologías en el ámbito judicial. En particular, es imperativo reconocer la relevancia de la **protección de la privacidad** y la **intimidad**, valores fundamentales que deben ser preservados en todas las etapas del proceso judicial. A continuación, se presentan una serie de **recomendaciones** fundamentales para garantizar que el **derecho a la intimidad** sea respetado y protegido dentro del sistema judicial, especialmente en un contexto donde los **delitos informáticos** y las vulneraciones de datos personales son cada vez más comunes.

1. Educación continua para los profesionales del derecho

En primer lugar, y como punto crucial para el fortalecimiento de la justicia digital, se recomienda que, considerando el marco de un **estado constitucional de derecho**, se implemente un programa de **educación continua** para todos los profesionales del derecho, especialmente aquellos que operan dentro de **juzgados unipersonales**. Esta educación debe estar orientada a mejorar la comprensión de los principios de **protección de datos personales**, **confidencialidad** y **seguridad de la información** en el contexto judicial. Es fundamental que los operadores jurídicos estén constantemente actualizados sobre las nuevas tecnologías, las normativas internacionales de protección de datos, así como los **desafíos legales y éticos** que surgen con la digitalización de la justicia.

El objetivo de esta formación es asegurar que los profesionales del derecho no solo comprendan las implicancias de su trabajo, sino que también sean capaces de manejar la información confidencial de manera responsable y respetuosa con los derechos fundamentales de las personas. De este modo, se garantizará que los derechos a la **intimidad** y la **protección de datos personales** sean adecuadamente resguardados, asegurando que la justicia no sea solo eficiente, sino también ética y respetuosa de las libertades individuales.

2. Protección continua de la intimidad en el contexto digital

Es necesario recalcar que la **intimidad** es un derecho fundamental, de rango constitucional, cuya protección debe ser una prioridad en el ámbito judicial. Este derecho

debe ser preservado constantemente, especialmente en un contexto de creciente **vulnerabilidad digital**. En particular, los **delitos informáticos**, tales como el acceso no autorizado a sistemas judiciales, la alteración de datos o la divulgación ilegal de información personal, constituyen una seria amenaza para la **intimidad** de los individuos y, por ende, deben ser abordados con la máxima seriedad.

Los **operadores de derecho**, como jueces, fiscales y abogados, deben ser conscientes de que las acciones ilícitas que vulneran la intimidad de las personas, apoyadas en tecnologías digitales, pueden tener un impacto devastador sobre la **dignidad humana**. Los ataques a la **confidencialidad** de los datos personales no solo infringen la privacidad, sino que también socavan el **honor** y la **seguridad** de las personas involucradas. Por ello, es esencial que los profesionales del derecho actúen con la mayor cautela y responsabilidad en relación con la protección de la información confidencial que se maneja dentro de los tribunales.

3. Conciliación del derecho a la información y el respeto a la intimidad

Otro aspecto clave que debe ser tomado en cuenta es la necesidad de **conciliar el derecho a la información** con la **protección de la intimidad** personal. En un mundo donde el acceso a la información es crucial para el **funcionamiento democrático** y la **transparencia judicial**, los **profesionales del derecho** deben asegurarse de que el derecho a ser informado no interfiera con el derecho de los individuos a **mantener su intimidad** y su **dignidad**.

Es fundamental que los sistemas judiciales respeten las normativas que limitan la divulgación de **información personal** confidencial. Si bien es cierto que los **datos personales** pueden ser esenciales para la administración de justicia, su **uso** debe estar estrictamente regulado para evitar que se utilicen con fines **lucrativos** o para **explotar** la vulnerabilidad de las personas. En este sentido, los **profesionales del derecho**, especialmente aquellos en juzgados unipersonales, deben estar bien preparados para identificar cuándo la **obtención de información** puede vulnerar el derecho a la **dignidad** y la **moralidad** de los individuos.

La **formulación clara de límites** en cuanto al acceso y la utilización de información sensible debe ser parte fundamental de las políticas judiciales, siempre garantizando que cualquier uso de la información personal sea legítimo, ético y realizado

con el **consentimiento** de los implicados, siempre que no se comprometan otros principios fundamentales del derecho.

4. Garantizar la integridad de los datos y la confidencialidad en los sistemas judiciales

La implementación de medidas de **protección de datos** debe ser vista como un imperativo dentro de los sistemas judiciales. Los **principios de confidencialidad** y **seguridad** en el manejo de la información no son solo una obligación legal, sino también una cuestión ética que asegura la **integridad** de la administración de justicia. En un contexto donde los datos se gestionan y transmiten principalmente en formato digital, los **profesionales del derecho** deben ser conscientes de la importancia de **resguardar** los datos personales, tanto en su **almacenamiento** como en su **transmisión**.

El **principio de difusión de la información** en el ámbito judicial, aunque esencial para la transparencia, debe ser **equilibrado** cuidadosamente con el derecho a la **privacidad**. En este sentido, la **confidencialidad** debe ser considerada una **excepción** cuando los datos personales o los documentos sensibles no estén relacionados directamente con la **justicia pública** o la **toma de decisiones judiciales**. Por ello, se deben establecer **protocolos estrictos de acceso** a la información, **sistemas de encriptación** avanzados para los archivos judiciales y una **supervisión constante** de las plataformas tecnológicas utilizadas en el proceso judicial.

Los **principios de seguridad y protección de datos** no deben ser tratados como un tema secundario, sino que deben estar **integrados** en la estructura misma del sistema judicial. Es crucial que los profesionales del derecho, desde los **jueces** hasta los **administradores de los tribunales**, sean responsables de mantener y aplicar estos principios con el fin de garantizar que la **información personal** de las personas involucradas en los casos judiciales no se vea comprometida.

5. Promoción de un entorno seguro para el acceso a la justicia

Finalmente, el principio de **acceso a la justicia** debe ser considerado de manera integral dentro de cualquier sistema judicial digital. El acceso a la justicia no solo implica la capacidad de los ciudadanos para presentar sus casos ante los tribunales, sino también la **protección** de sus **derechos fundamentales** a lo largo de todo el proceso. Este principio debe ser promovido a través de la creación de plataformas **accesibles** y **seguros**, que garanticen que **todos los individuos**, independientemente de su estatus social o su

capacidad tecnológica, puedan acceder a un **proceso judicial transparente, justo y libre de vulneraciones de su privacidad**.

Las políticas que fomenten la **digitalización** de la justicia deben tener en cuenta las **desigualdades sociales y tecnológicas**, asegurando que el **acceso a la justicia** no esté limitado por la **falta de recursos** tecnológicos o la **ignorancia digital**. En este sentido, es esencial que los sistemas judiciales digitales estén diseñados para ser **inclusivos**, ofreciendo **asistencia técnica** y **orientación jurídica** para aquellos que no tienen los conocimientos necesarios para interactuar con las plataformas digitales.

Las recomendaciones aquí presentadas subrayan la importancia de una aproximación integral y bien pensada para la protección de los derechos fundamentales en el contexto de un sistema judicial digitalizado. Si bien la tecnología ofrece una oportunidad única para **mejorar la eficiencia** y **accesibilidad** de los procesos judiciales, también plantea **retos significativos** en términos de **protección de datos** y **seguridad**. Es por ello que la **educación continua**, el **fortalecimiento de la confidencialidad** y la **implementación de sistemas seguros** deben ser considerados no solo como medidas de protección, sino como componentes esenciales para garantizar que la justicia digital no solo sea **eficaz**, sino también **ética**, **justa** y **respetuosa de los derechos fundamentales** de todas las personas.

REFERENCIAS

Acurio del Pino, S. (2012). "Delitos Informáticos": Generalidades. Recuperado de: http://www.oas.org/JURÍDICO/spanish/cyb_ecu_delitos_in form.pdf.

Amaya, T., Avalos, A. y Jule F. (2012). *Derecho a la Intimidad en la estructura de la ley especial de intervención de telecomunicaciones*. Para optar el grado de Licenciado en Ciencias Jurídicas. Universidad de El Salvador, San Salvador.

Bernal, C., (2006). Metodología de la Investigación para administración, economía, humanidades y ciencias sociales. (3° ed.). Bogotá: Pearson Educación.

Beshar, R., D. (2008). Metodología de la Investigación. Editorial Shalom.

Blossiers, H., J. (2003). *Criminalidad Informática.* Lima: Edit. Librería Portocarrero.

Bradanovic, P., T. (2006). Conceptos básicos de seguridad informática. Chile

Bramont – Arias, T., L. (1997). El Delito Informático en el Código Penal Peruano. Lima, Perú. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Canahuire, A. Endara, F. y Morante, E. (2015). ¿Cómo hacer la tesis universitaria? Una guía para investigadores. Cuzco: Colorgraf.

Castro, A. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. NOVUM JUS 10 (1). (enero - junio 2016). 113-133. Consultado el 5 de junio del 2021. ISSN: 1692-6013. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/16407/1/Derecho%20a%20la%20intimidad%20en%20las%20redes%20sociales%20de%20internet%20en%20Colombia.pdf

Celis (2006). La Protección de la Intimidad como Derecho Fundamental de los mexicanos. En D. Cienfuegos y M. Macías. Autores (eds.), Protección de la persona y derechos fundamentales (pp. 71–108). México: UNAM

Espinoza, M., J. (2008). Validación y estandarización de instrumentos. Recuperado de: http://extension.upbbga.edu.co/web2/pagina2/archivos/VYEInstrumentos.pdf

Ferro V., J. (2016). Seguridad Informática: Aspectos Generales y Especiales. España: Autoediciones Tagus.

Fernández, T. (2012). Diseño del trabajo de investigación. Trujillo: Universidad Cesar Vallejo.

Ferreira, R. D. (1982). El Derecho a la Intimidad Análisis del artículo 1071 bis del Código Civil: A la luz de la doctrina, la legislación comparada y la jurisprudencia. Editorial Universidad, Buenos Aires.

Gonzales, J. (2013) Tesis: Delincuencia Informática: Daños Informáticos del Art. 264 del Código Penal y Propuesta de Reforma. Para optar el Título de Doctor en Derecho. Presentada en la Universidad Complutense de Madrid. España.

Gonzales, E. (2015). Privacidad en Internet: Los Derechos Fundamentales de privacidad e intimidad e internet y su regulación jurídica. La vigilancia masiva. [Tesis doctoral, Universidad Castilla de la Mancha de Madrid], Repositorio Institucional de la UCLM. https://ruidera.uclm.es/xmlui/bitstream/h5andle/10578/10092/TESIS%20Gonz%C3%A1lez%20Porras.pdf?sequence=1&isAllowed=y

Guzmán, M. (2013) Tesis: El derecho fundamental a la "protección de datos" personales en México: Análisis desde la influencia del ordenamiento jurídico español. Para optar el Título de Doctor en Derecho. Presentada en la Universidad Complutense de Madrid. España.

Hernández, O., E. (sf.) Seguridad y privacidad en los "Delitos Informáticos". Recuperado de: www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF

Hernández, M., A. (2004). Tesis: Los Delitos a través del uso de la Computadora. México. Para obtener el Título de Abogado. Presentada en la Universidad Autónoma de San Luis de Potosí. Bolivia.

Hernández, R., Fernández, C., Baptista, M. (2014). Metodología de la Investigación. Sexta Edición. México. Interamericana Editores S.A de C.V.

Hurtado, P., J. y Prado, S., V. (2011). Manual del Derecho Penal – Parte General. 4ta. Edición. Lima – Perú. Editorial Moreno S.A. Tomo I 686 pág. Tomo II.

Ivo, D. (2013). La ponderación entre los conflictos de la libertad de expresión y el derecho a la vida privada: estudio jurisprudencial entre dos culturas. Universidad de los

Andes - Facultad de Derecho - Revista de Derecho Público. Número 30. (Enero – junio 2013). Consultado el 21 de junio del 2021. Disponible en: https://derechopublico.uniandes.edu.co/components/com_r evista/archivos /derecho pub/pub366.pdf

Martínez, M. (2016). La Investigación Cualitativa. Revista de Investigación en Psicología, 20.

Ministerio de Justicia (22 de marzo del 2013). D.S. 003- 2013- JUS

Ministerio Público (2017). Boletín estadístico del Ministerio Público. Recuperado de: http://www.mpfn.gob.pe.

Núñez, P., J. (1996). Derecho Informático. Lima, Perú. Editores MARSOL Perú.

ONU (2018). Resolución sobre el derecho a la privacidad en la era digital. Consultado el 13 de junio del 2021. Disponible en https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/E6ABB50700326D61052586DF00709364/$FILE/A_RES_73_179_S.pdf

Poder Judicial del Perú. Acuerdo plenario N.º 03-2006-CJ/116. Delitos contra el honor personal y derecho constitucional al derecho de expresión y de información. Recuperado de: https://www.pj.gob.pe/wps/wcm/connect/1e3604004075bad5b75ff799ab657107/acuerdo_plenario_03-2006_CJ_116.pdf?MOD=AJPERES&CACHEID=1e3604004075bad5b75ff799ab657107

Polit DF, Hungler BP. (2018). Introducción a la investigación en ciencias de la salud". En: Polit DF, Hungler BP. Investigación científica en ciencias de la salud. 6ª ed. México: McGraw-Hill Interamericana.

Proyecto de ley 7222/ 2020- CR. (26 de febrero del 2021). Ley que regula el uso indebido de medios tecnológicos en telecomunicaciones como las redes sociales y aplicación. Congreso de la República. https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL07222-20210226.pdf

Reátegui, J. (2009). Derecho Penal – Parte General. Lima, Perú. Gaceta Jurídica S. A.

Reyna, L., M. (abril 2001). El bien jurídico en el delito informático. Lima: revista electrónica de derecho informático, Alfa – Redi, Nro. 33.

Reyna, L., M. (2002). Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima – Perú. Juristas Editores.

Relat, M. (2010). Revisiones Temáticas Introducción a la investigación

básica. RADP online. 33 (3). 221- 227. Consultado el 08 de junio del 2021.Disponible en: https://www.researchgate.net/publication/341343398_Introduc_cion_a_la_Investigacion_basica

Reyna, L., M. (abril 2001). El bien jurídico en el delito informático. Lima: revista electrónica de derecho informático, Alfa – Redi, Nro. 33.

Reyna, L., M. (2002). Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima – Perú. Juristas Editores.

Riascos, L. (1999) Tesis: El "Derecho a la Intimidad", la visión iusinformatica y el delito de los datos personales. Para optar el Título de Doctor en Derecho. Presentada en la Universidad de Lleida, España. España.

Rojas, T., R. & Ameghino, C., Z. (2002). Derecho Informático. Ediciones Flores.

Rojas, M. (2015). Las Nuevas Formas de Materialización de la Libertad de Expresión y la Vulneración del Derecho a la Intimidad de la

Persona. [Tesis doctoral, Universidad Nacional de Trujillo]. Repositorio UNT. https://dspace.unitru.edu.pe/handle/UNITRU/5733

Sáenz, C., J. (2002). "Delitos Informáticos" o Delitos Cometidos por medios informáticos. Argentina. Revista de Derecho Informático Alfa – Redi, Nro. 45.

Silva, S., J. (2006). La expansión del derecho penal: Aspectos de la política Criminal en las sociedades Postindustriales. Buenos Aires Argentina. Editorial Euros Editores S.R.L. https://dialnet.unirioja.es/servlet/autor?codigo=48676

Téllez, V., J. (1991). Derecho informático. México. Universidad autónoma de México.

Tribunal Constitucional del Perú (2005). Exp. Nº 6712-2005-HC/TC. Caso Magaly Jesús Median Vela y Ney Guerrero Orellana. Recuperado de: https://tc.gob.pe/jurisprudencia/2006/06712-2005-HC.pdf

Tribunal Constitucional del Perú (2005). STC 1417-2005-PA/TC. Caso Manuel Anicama Hernández. Recuperado de: https://tc.gob.pe/jurisprudencia/2005/01417-2005-AA.pdf

Tribunal Constitucional del Perú (2005). STC 5854-2005-PA/TC. Caso Pedro Andrés Lizama Puelle y Jurado Nacional de Elecciones. Recuperado de: https://tc.gob.pe/jurisprudencia/2005/05854-2005-AA.pdf

Tribunal Constitucional del Perú (2004). STC Nº 00004-2004-AI/TC. Caso Colegio de Abogados del Cusco y otros. Recuperado de: https://tc.gob.pe/jurisprudencia/2004/00004-2004-AI%20Resolucion.html

Tribunal Constitucional del Perú (2005). STC Nº 00009-2014-AI/TC. Más de cinco mil ciudadanos contra la ley 29720. Recuperado de: https://tc.gob.pe/jurisprudencia/2016/00009-2014-AI.pdf

Valderrama, S. (2007). Pasos para elaborar proyectos y tesis de investigación científica. México: Trillas.

Villanueva, A. (2016). El derecho al honor, a la intimidad y a la propia imagen, y su choque con el derecho a la libertad de expresión e información en el ordenamiento jurídico español. DIKAION, 25, 2 (2016). 190- 215. DOI: 10.5294/DIKA.2016.25.2.3. Consultado el 29 de junio del 2021. Disponible en: http://dikaion.unisabana.edu.co/index.php/dikaion/article/view/6508/4457

Villavicencio, T., F. (2014). "Delitos Informáticos". Perú. Revista IUS VERITAS, Nro.49.

Volpato, S. (2016). El derecho a la intimidad y las nuevas tecnologías de información. (Tesis doctoral inédita). Universidad de Sevilla, Sevilla.

Zevallos, E. (2013) Tesis: La "protección de datos" personales en España: Evolución normativa y criterios de aplicación. Para optar el Título de Doctor en Derecho. Presentada en la Universidad Complutense de Madrid. Madrid, España.

Zorrilla, A., S. (1993). Introducción a la metodología de la investigación. (11 ed.). México: Aguilar y León Cal Editores.