



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América
Facultad de Derecho y Ciencia Política
Escuela Profesional de Derecho

**La protección de datos personales y su relación con los
derechos digitales en la legislación peruana**

TESIS

Para optar el Título Profesional de Abogado

AUTOR

Jorge Vladimir AGUILAR HERNANDO

ASESOR

Dr, Pedro Gustavo Alberto CUETO CHUMAN

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Aguila, J. (2024). *La protección de datos personales y su relación con los derechos digitales en la legislación peruana*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Derecho y Ciencia Política, Escuela Profesional de Derecho]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios: autor / asesor

Datos de autor	
Nombres y apellidos	Jorge Vladimir Aguilar Hernando
Tipo de documento de identidad	DNI
Número de documento de identidad	707973691
URL de ORCID	https://orcid.org/0000-0002-4652-2774
Datos de asesor	
Nombres y apellidos	Pedro Gustavo Alberto Cueto Chuman
Tipo de documento de identidad	DNI
Número de documento de identidad	08865971
URL de ORCID	https://orcid.org/0000-0002-0492-8952
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	José Félix Palomino Manchego
Tipo de documento de identidad	DNI
Número de documento de identidad	06756703
Miembro del jurado 1	
Nombres y apellidos	Clotilde Cristina Vigil De Quiroz
Tipo de documento de identidad	DNI
Número de documento de identidad	16644992
Miembro del jurado 2	
Nombres y apellidos	Julio Hernán Figueroa Bustamante
Tipo de documento de identidad	DNI
Número de documento de identidad	08248540
Miembro del jurado 3	
Nombres y apellidos	Jorge Adalberto Pérez López
Tipo de documento de identidad	DNI
Número de documento de identidad	08162135

Datos de investigación	
Línea de investigación	E.1.3.5 Ciencias Informáticas E.1.3.5 Gestión Pública
Grupo de investigación	Entidades Publicas y Privadas de Lima.
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Latitud: -12.056445 Longitud: -77.085994
Año o rango de años en que se realizó la investigación	2023-2024
URL de disciplinas OCDE	Derecho https://purl.org/pe-repo/ocde/ford#5.05.01 Administración pública https://purl.org/pe-repo/ocde/ford#5.06.02



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE DERECHO Y CIENCIA POLÍTICA

**ACTA DE EXAMEN ORAL PRESENCIAL PARA EL OTORGAMIENTO DEL TÍTULO
PROFESIONAL DE ABOGADO CON SUSTENTACIÓN DE TESIS**

N°027

Reunido el Jurado Examinador, constituido por los señores profesores:

- 1.-PRESIDENTE: Dr. JOSÉ FÉLIX PALOMINO MANCHEGO
- 2.- Mg. CLOTILDE CRISTINA VIGIL CURO DE QUIROZ
- 3.- Mg. JULIO HERNÁN FIGUEROA BUSTAMANTE
- 4.- Mg. JORGE ADALBERTO PÉREZ LÓPEZ
- 4.- Abg. PEDRO GUSTAVO ALBERTO CUETO CHUMAN (ASESOR)

El bachiller postulante al Título Profesional de Abogado, don:

JORGE VLADIMIR AGUILAR HERNANDO

Procedió la sustentación de su tesis titulado:

La protección de datos personales y su relación con los derechos digitales en la legislación peruana

En la redacción del examen escrito de fin de carrera, el graduando fue aprobado con la nota de

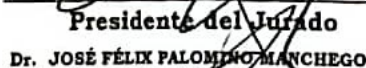
TRECE (13)

Concluida la prueba oral, se practicó la votación correspondiente, resultando el candidato:

**APROBADO POR UNANIMIDAD Y CON MAYORES
HONORES CON LA NOTA DE VEINTE (20)**

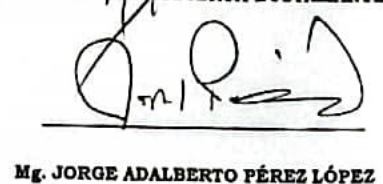
Y para constancia se le extiende la presente Acta, en Lima a los VEINTICUATRO días del mes de SETIEMBRE del año 2024.


Mg. CLOTILDE CRISTINA VIGIL CURO DE QUIROZ


Presidente del Jurado
Dr. JOSÉ FÉLIX PALOMINO MANCHEGO


Mg. JULIO HERNÁN FIGUEROA BUSTAMANTE


Abg. PEDRO GUSTAVO ALBERTO CUETO CHUMAN
(ASESOR)


Mg. JORGE ADALBERTO PÉREZ LÓPEZ

CERTIFICADO DE SIMILITUD

Yo, **Pedro Gustavo Alberto Cueto Chuman** en mi condición de asesor acreditado con la Resolución Directoral **N°000291-2023-EPD-FDCP/UNMSM** de la tesis, cuyo título es "**La protección de datos personales y su relación con los derechos digitales en la legislación peruana**", presentado por el bachiller **Jorge Vladimir Aguilar Hernando** para optar el título profesional de abogado.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de **20%** de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del Asesor

DNI: **08865971**

Nombres y apellidos del asesor:

Pedro Gustavo Alberto Cueto Chuman



Huella Digital

DEDICATORIA:

Dedico esta investigación a mis madres: Nila, Crispina, Mercedes, Nelly y mi familia por el apoyo incondicional brindado en el desarrollo de este trabajo.

AGRADECIMIENTOS:

Agradezco a mi Alma Mater por las enseñanzas recibidas a lo largo de mi estancia por los claustros universitarios, a mi asesor que me guio en el camino de la investigación dándome orientaciones oportunas para el desarrollo del presente trabajo.

ÍNDICE DE CONTENIDO

DEDICATORIA:	ii
AGRADECIMIENTOS:	iii
ÍNDICE DE CONTENIDO	iv
ÍNDICE DE TABLAS	viii
ÍNDICE DE FIGURAS	ix
RESUMEN	x
ABSTRACT	xii
I. INTRODUCCION	1
I.1. Introducción	1
I.2. Planteamiento del problema	2
• Determinación del problema	2
• Formulación del problema	6
I.3. Objetivo	7
I.4. Importancia y alcance de la investigación	8
I.5. Limitaciones de la investigación	10
II. REVISION DE LITERATURA	18

II.1.	Marco Teórico	18
II.2.	Antecedentes del estudio	29
II.3.	Bases Teóricas	46
II.4.	Definición de Términos	68
III.	HIPOTESIS Y VARIABLES	83
III.1.	Hipótesis.....	83
III.2.	Variables.....	84
III.3.	Operacionalización de las variables	86
IV.	MATERIALES Y METODOS	90
IV.1.	Área de estudio	90
IV.2.	Diseño de Investigación	90
IV.3.	Población y muestra	93
IV.4.	Procedimientos, técnicas e instrumentos de recolección de información.....	94
IV.5.	Análisis estadístico	98
V.	RESULTADOS	101
V.1.	Presentación y análisis de resultados	101
VI.	DISCUSIÓN.....	112

VII. CONCLUSIONES Y RECOMENDACIONES.....	133
Conclusiones	133
Recomendaciones	140
VIII. PROPUESTA.....	149
VIII.1. Introducción.....	149
VIII.2. Problemática	150
VIII.3. Objetivos de la propuesta	151
VIII.4. Análisis SEPTE	152
VIII.5. Propuesta de Marco legal respecto a la Educación Digital y Protección de Datos en el Perú - Exposición de Motivos	154
VIII.6. Propuesta de ley de educación digital y protección de datos	158
VIII.7. Propuesta de Reglamento de Ley respecto a la educación digital y protección de datos	160
BIBLIOGRAFIA	164
ANEXOS	180
Anexo 1: Matriz de consistencia	181
Anexo 2: Matriz de Operacionalización variable Protección de datos personales	183

Anexo 3: Matriz de Operacionalización variable Derechos Digitales	185
Anexo 4: Declaración de Originalidad del Asesor	187
Anexo 5: Declaración de Originalidad del Autor.....	189
Anexo 6: Formato de Encuesta	190

ÍNDICE DE TABLAS

Tabla 1 Niveles de frecuencia y porcentajes sobre la Protección de los datos personales y los derechos digitales.....	102
Tabla 2 Niveles de frecuencia y porcentajes sobre la Privacidad y confidencialidad.....	103
Tabla 3 Niveles de frecuencia y porcentajes sobre el derecho al olvido	104
Tabla 4 Niveles de frecuencia y porcentajes sobre el derecho a la identidad digital.....	105
Tabla 5 Niveles de frecuencia y porcentajes sobre el derecho a la educación digital.....	106
Tabla 6 Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derechos digitales.....	107
Tabla 7 Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Privacidad y confidencialidad	108
Tabla 8 Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derecho al olvido	109
Tabla 9 Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derecho a la identidad digital.....	110
Tabla 10 Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derecho a la educación digital	111

ÍNDICE DE FIGURAS

Figura 1	Protección de los datos personales y los derechos digitales.....	102
Figura 2	Percepción sobre la Privacidad y confidencialidad.....	103
Figura 3	Percepción sobre el derecho al olvido.....	104
Figura 4	Percepción sobre el derecho a la identidad digital	105
Figura 5	Percepción sobre el derecho a la educación digital	106

RESUMEN

El presente trabajo de investigación tuvo como objetivo principal determinar la relación entre la protección de datos personales y los derechos digitales en el contexto peruano. En relación con la parte metodológica fue de tipo básica, con un enfoque cuantitativo y fue trabajado con un diseño descriptivo correlacional. El diseño de la investigación es no experimental, corte transversal. La muestra estuvo constituida por 378 ciudadanos. Asimismo se aplicó los instrumentos de cuestionario el mismo que fue distribuido de forma electrónica. Para el análisis estadístico de los datos se utilizó la herramienta SPSS versión 26.

El estudio se propone abordar de manera exhaustiva la intersección entre la protección de datos personales y los derechos digitales en Perú, centrándose en aspectos clave como la privacidad, el olvido digital, la identidad y la educación digital. La hipótesis general, respaldada por el análisis estadístico (Rho de Spearman 0,615), sostiene que existe una relación significativa entre la protección de datos personales y los derechos digitales en el Perú. Este hallazgo sugiere la importancia de considerar la protección de datos como un elemento crucial en la garantía y promoción de los derechos digitales en el entorno peruano.

Este resultado subraya la relevancia de la protección de datos como un componente esencial en el aseguramiento y fomento de los derechos digitales en el contexto peruano. La salvaguarda de datos personales y el ejercicio pleno de los derechos digitales es un punto crítico tanto en organizaciones públicas o privadas, destacando que la preservación de la privacidad y la seguridad de la

información personal se correlaciona directamente con la capacidad de los individuos para disfrutar de sus derechos en el ámbito digital.

Este resultado refuerza la necesidad de estrategias integrales y normativas robustas que no solo aborden la protección de datos desde una perspectiva legal, sino que también promuevan prácticas y políticas organizacionales que refuercen la relación intrínseca entre la protección de datos y la experiencia digital de los ciudadanos. Además, evidencia la importancia de un enfoque proactivo que anticipe los desafíos emergentes de la protección de datos y los derechos digitales, destacando así la urgencia de medidas preventivas orientadas a la educación digital y soluciones efectivas para garantizar un entorno digital seguro y respetuoso en el Perú.

Palabras Clave: Protección de datos, derechos digitales, derecho al olvido digital, privacidad y confidencialidad digital, identidad digital, educación digital

ABSTRACT

The main objective of this research work was to determine the relationship between personal data protection and digital rights in the Peruvian context. In relation to the methodological part, it was of a basic type, with a quantitative approach and was worked with a correlational descriptive design. The research design is non-experimental, cross-sectional. The sample consisted of 378 citizens. Likewise, the questionnaire instruments were applied, which were distributed electronically. For the statistical analysis of the data, the SPSS version 26 tool was used.

The study aims to comprehensively address the intersection between personal data protection and digital rights in Peru, focusing on key aspects such as privacy, digital forgetting, identity and digital education. The general hypothesis, supported by statistical analysis (Spearman's Rho 0.615), holds that there is a significant relationship between personal data protection and digital rights in Peru. This finding suggests the importance of considering data protection as a crucial element in the guarantee and promotion of digital rights in the Peruvian environment.

This result underlines the relevance of data protection as an essential component in the assurance and promotion of digital rights in the Peruvian context. The safeguarding of personal data and the full exercise of digital rights is a critical point in both public and private organizations, highlighting that the preservation of the privacy and security of personal information directly correlates with the ability of individuals to enjoy their rights in the digital realm.

This result reinforces the need for comprehensive strategies and robust regulations that not only address data protection from a legal perspective, but also promote organizational practices and policies that reinforce the intrinsic relationship between data protection and citizens' digital experience. In addition, it highlights the importance of a proactive approach that anticipates the emerging challenges of data protection and digital rights, thus highlighting the urgency of preventive measures aimed at digital education and effective solutions to ensure a safe and respectful digital environment in Peru.

Keywords: Data protection, digital rights, right to be forgotten digitally, digital privacy and confidentiality, digital identity, digital education

I. INTRODUCCION

I.1. Introducción

En la era digital en la que la sociedad se desarrolla, las vidas de las personas se han entrelazado profundamente con la tecnología. Desde las interacciones en redes sociales hasta las compras en línea, diariamente se genera y comparte una gran cantidad de información personal en el ciberespacio (Kirchschlaeger, 2019). Sin embargo, esta creciente dependencia de la tecnología también conlleva una creciente preocupación por la protección de los datos personales y la garantía de los derechos digitales (Moreno Bobadilla, 2020a).

La protección de datos personales se erigió como un pilar fundamental en la agenda de la privacidad y la seguridad en línea. Cada vez más, tanto individuos como empresas e instituciones gubernamentales reconocieron la importancia de salvaguardar la información personal de las personas, evitando el acceso no autorizado, el uso indebido y la divulgación no deseada (Bello, 2021). A medida que las amenazas cibernéticas evolucionan, se hace imprescindible adoptar medidas sólidas para preservar la confidencialidad, integridad y disponibilidad de los datos en el entorno digital (Berdote, 2022).

Simultáneamente, garantizar los derechos digitales de los usuarios se volvió un desafío esencial en una sociedad altamente interconectada. Estos derechos comprendían aspectos como la privacidad, la libertad de expresión, el acceso a la información y la no discriminación en línea. Con el desarrollo continuo de la tecnología, encontrar un equilibrio entre la innovación y la

protección de los derechos fundamentales se convirtió en una prioridad vital para la sociedad (Wagner et al., 2020).

En esta era de constante transformación digital, la comprensión de la importancia de proteger los datos personales y salvaguardar los derechos digitales se tornó esencial para crear un entorno en línea seguro y confiable para todos (Serna, 2021e). Este conocimiento permitiría a las personas navegar por el mundo digital con confianza y conciencia, y enfrentar los desafíos que surgieran en el camino (Rochel, 2021).

En el presente trabajo de investigación, se analizó la relación que los principios fundamentales de la protección de datos personales, los marcos regulatorios que regían esta área y las mejores prácticas establecidas para garantizar la seguridad y privacidad en línea. También se analizó los derechos digitales que deben protegerse y cómo cada individuo debe contribuir a la construcción de un entorno digital más seguro y respetuoso de los derechos fundamentales.

I.2. Planteamiento del problema

- **Determinación del problema**

A nivel internacional existen problemas derivados de las brechas en la regulación de datos entre comunidades autónomas o estados que son un desafío en países con sistemas descentralizados, como es el caso de España o Estados Unidos de América (Duque, 2019). Esto se debe a que cada comunidad autónoma o estado puede tener sus propias normativas y leyes relacionadas con la

protección de datos, lo que puede generar discrepancias y confusiones para las empresas y ciudadanos que operan en diferentes regiones del país. Esta falta de armonización puede dificultar la implementación coherente de políticas de protección de datos y la cooperación efectiva entre distintas autoridades que ejercen supervisión sobre los mismos (Maréchal & Project, 2015).

En América Latina, existen varios problemas relacionados con la protección de datos personales y los derechos digitales. Estos problemas incluyen deficiencias en la seguridad de datos en empresas, baja conciencia sobre la privacidad, acceso no autorizado a datos personales, uso indebido de datos con fines delictivos, escaso control sobre la privacidad en plataformas digitales locales y limitaciones en el acceso a información pública en línea (Porcelli, 2019). Para abordar estos problemas, es esencial fortalecer la regulación y concientización sobre la protección de datos, implementar medidas de seguridad adecuadas y promover prácticas responsables en el manejo de información personal. Además, es necesario fomentar una cultura de transparencia y acceso a la información para garantizar el ejercicio efectivo de los derechos digitales en la región (Rank & Berberi, 2022).

Tal es el caso que en Colombia, se identifica que uno de los problemas fundamentales en relación con la protección de datos personales es la referida a la existencia de deficiencias en la seguridad de datos en empresas. Esto significa que muchas organizaciones no implementan las medidas de seguridad adecuadas para proteger la información personal de sus usuarios o clientes. La falta de sistemas de encriptación, protección contra ciberataques y protocolos de

acceso seguro, entre otros, puede exponer los datos personales a amenazas externas y violaciones de privacidad (Hernandez Palma, 2022).

En Brasil, el acceso no autorizado a datos personales por terceros es un problema significativo. Esto ocurre debido a vulnerabilidades en los sistemas de seguridad de las empresas, ataques informáticos o incluso mediante la recopilación de información por parte de terceros sin el consentimiento explícito de los usuarios. Esta situación ha expuesto a los individuos a violaciones de privacidad y poner en riesgo la confidencialidad de sus datos (Aponte, 2022).

En México, el uso indebido de datos personales con fines de extorsión es un grave problema. Los ciberdelincuentes obtienen información personal sensible y la utilizan para extorsionar a las víctimas, amenazándolas con divulgar la información o utilizarla para obtener un beneficio económico ilícito (Bizberge et al., 2020)

A nivel nacional, en nuestro país, se identifican diversos problemas relacionados con la protección de datos personales, los cuales han sido objeto de análisis y preocupación. En primer lugar, la carencia de una legislación integral de protección de datos ha generado ambigüedades y vacíos legales en cuanto a la salvaguarda de la privacidad y seguridad de la información personal (Ley N° 29733). La ausencia de un marco legal sólido que defina los derechos y responsabilidades de las partes involucradas en el tratamiento de datos personales, así como las sanciones por incumplimiento, ha dificultado la implementación de medidas de protección y ha puesto en riesgo los derechos digitales de los ciudadanos (Rodríguez, 2022).

Por otro lado, la vulnerabilidad de los datos en instituciones públicas y privadas constituye un riesgo considerable para la privacidad y seguridad de los ciudadanos. La falta de medidas de seguridad adecuadas, como la encriptación de datos, la protección de acceso y la gestión de riesgos, ha dejado a estas entidades susceptibles a ciberataques y violaciones de datos (Chupillón Monsalve & Vallejos Huamán, 2018). Esto ha afectado no solo a los ciudadanos cuyos datos se encuentran en riesgo, sino también ha mermado la confianza del público hacia las instituciones que almacenan y procesan información personal. (Resolución Ministerial N° 070-2013-PCM, Reglamento de Seguridad de las Tecnologías de la Información y Ley N° 30096, Ley de Delitos Informáticos)

Además, la escasez de recursos financieros y tecnológicos ha sido un obstáculo para implementar medidas de seguridad efectivas en el manejo de datos personales (León et al., 2021). La adopción de tecnologías avanzadas de seguridad y la capacitación del personal en temas de ciberseguridad han requerido inversiones significativas que algunas instituciones y empresas no han podido realizar, debilitando así las capacidades para proteger los datos y mitigar riesgos de vulnerabilidades en el entorno digital. La misma que debe ser presupuestada en la Ley N° 28411, Ley General del Sistema Nacional de Presupuesto (Luna Cervantes, 2021a).

Otro problema importante se ha centrado en la poca transparencia en el uso de datos por parte de las instituciones gubernamentales y privadas. La falta de divulgación y claridad acerca de las prácticas de recolección y uso de datos ha generado desconfianza y preocupaciones en la población en cuanto al respeto de sus derechos digitales. Es vital que los ciudadanos estén informados

sobre cómo se utilizan sus datos personales, especialmente cuando provienen de fuentes gubernamentales. La falta de transparencia ha dificultado la rendición de cuentas y la participación ciudadana en la toma de decisiones respecto al uso de la información personal. Esto conforme a la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública. Y Decreto Supremo N° 043-2003-PCM, Reglamento de la Ley de Transparencia y Acceso a la Información Pública (Garcia & Perea, 2020).

- **Formulación del problema**

Tomando en consideración la información reseñada precedentemente se planteó los siguientes problemas:

Problema General

¿Cómo la protección de datos personales se relaciona con los derechos digitales en el Perú?

Problemas específicos

Problema Especifico 1

¿Cómo la protección de datos personales se relaciona con la privacidad y confidencialidad digital en el Perú?,

Problema Especifico 2

¿Cómo la protección de datos personales se relaciona con el derecho al olvido digital en el Perú?,

Problema Especifico 3

¿Cómo la protección de datos personales se relaciona con el derecho a la identidad digital en el Perú?

Problema Especifico 4

¿Cómo la protección de datos personales se relaciona con el derecho a la educación digital en el Perú?

I.3. Objetivo

Tomando en consideración la información reseñada se planteó los siguientes problemas:

Objetivo General

Determinar cómo la protección de datos personales se relaciona con los derechos digitales en el Perú

Objetivos específicos

Objetivo Especifico 1

Determinar cómo la protección de datos personales se relaciona con la privacidad y confidencialidad digital en el Perú

Objetivo Especifico 2

Determinar cómo la protección de datos personales se relaciona con el derecho al olvido digital en el Perú

Objetivo Especifico 3

Determinar cómo la protección de datos personales se relaciona con el derecho a la identidad digital en el Perú

Objetivo Especifico 4

Determinar cómo la protección de datos personales se relaciona con el derecho a la educación digital en el Perú

I.4. Importancia y alcance de la investigación

El presente trabajo de investigación basa su justificación Teórica en que la protección de datos personales y su relación con los derechos digitales son cuestiones fundamentales en el entorno legal y tecnológico actual. Desde un punto de vista teórico, esta investigación se apoya en las teorías legales y de derechos humanos, así como en las teorías de la tecnología de la información y la privacidad. La legislación peruana, al igual que muchas jurisdicciones en todo el mundo, ha tenido que adaptarse para abordar los desafíos que plantea la era digital, y esta tesis se basa en la necesidad de comprender cómo las leyes de protección de datos se relacionan con la protección de los derechos digitales.

Asimismo la justificación metodológica se sostiene en que el enfoque de esta investigación es cuantitativo y correlacional simple, lo que se justifica por la necesidad de cuantificar y analizar las relaciones entre la protección de datos personales y los derechos digitales en el contexto peruano. La metodología cuantitativa permitirá la recopilación de datos numéricos que pueden ser analizados estadísticamente para identificar correlaciones significativas. La

correlación simple se selecciona porque se buscará determinar si existe una relación lineal entre estas dos variables. El uso de encuestas, análisis de legislación y datos estadísticos proporcionará un marco sólido para medir y evaluar las percepciones y prácticas relacionadas con la protección de datos y los derechos digitales en Perú.

La justificación práctica de esta investigación radica en su capacidad para informar y mejorar la legislación y las prácticas relacionadas con la protección de datos personales y los derechos digitales en Perú. La investigación podría arrojar información sobre las brechas existentes en la protección de datos y los desafíos en la protección de los derechos digitales en el entorno legal y tecnológico peruano. Estos hallazgos pueden tener un impacto directo en la toma de decisiones de legisladores, reguladores y empresas, y contribuir a un entorno más seguro y respetuoso de los derechos digitales en nuestro país.

La justificación social obedece a que en la era digital, la privacidad y la protección de datos personales son cuestiones que preocupan a la sociedad en su conjunto. La sociedad peruana se enfrenta a desafíos crecientes en lo que respecta a la gestión y protección de datos personales en línea. Una comprensión más profunda de cómo se relacionan estas cuestiones con los derechos digitales beneficiará a la sociedad al proporcionar una base para decisiones informadas y para exigir el respeto de sus derechos en línea.

Por último la justificación Tecnológica radica en que el avance de la tecnología digital ha llevado a la recopilación y procesamiento masivo de datos personales, lo que aumenta la importancia de la protección de la privacidad y la

seguridad en línea. La legislación y las políticas deben adaptarse a estas tecnologías emergentes para garantizar que los derechos digitales de los ciudadanos estén protegidos. La investigación aborda esta necesidad al explorar cómo la tecnología y la legislación interactúan en el contexto peruano y cómo pueden mejorarse para abordar los desafíos tecnológicos actuales y futuros.

I.5. Limitaciones de la investigación

En el marco de esta investigación que tuvo por finalidad examinar la interrelación entre la protección de datos personales y los derechos digitales en la legislación peruana, se hizo imperativo considerar las posibles limitaciones que podrían surgir. A continuación, se presentan las limitaciones que se identificaron en el desarrollo del presente trabajo:

En primer lugar, la recopilación de datos específicos y estadísticas vinculadas a violaciones de datos o incidentes de seguridad en el contexto peruano se ha enfrentado a desafíos significativos. La falta de información detallada ha limitado de manera notable la capacidad para realizar una evaluación precisa de la magnitud de estos problemas en el ámbito local. Esta carencia de datos específicos no solo ha dificultado el análisis cuantitativo, sino que también ha obstaculizado la comprensión profunda de la naturaleza y extensión de las violaciones de datos en el Perú. La ausencia de estadísticas pormenorizadas ha creado un vacío en la percepción de la situación, dejando interrogantes abiertas sobre la frecuencia, las tendencias y las consecuencias reales de estos incidentes en la seguridad de la información en el país. Este escenario subraya la necesidad apremiante de mejorar los mecanismos de

recopilación y difusión de datos relacionados con la seguridad de la información en el Perú, con el fin de dotar a los expertos, responsables de políticas y al ciudadano en general con información más precisa y completa para abordar efectivamente los desafíos emergentes en materia de protección de datos.

Un segundo aspecto para considerar fue la dinámica evolutiva de la legislación de protección de datos a lo largo del tiempo. La mutabilidad de las leyes, en su constante proceso de adaptación y actualización, ha influido significativamente en las investigaciones a largo plazo. Este factor, al ser una variable en constante cambio, ha introducido una complejidad adicional en la interpretación y coherencia de los resultados a lo largo de distintos periodos temporales. Con cada modificación legislativa, se redefine el marco normativo que regula la protección de datos. Esto no solo afecta la interpretación de los hallazgos de investigaciones anteriores, sino que también introduce nuevas consideraciones y matices en los estudios a medida que avanzan en el tiempo. La evolución de las leyes, si bien es esencial para mantenerse al día con los desafíos contemporáneos en la esfera digital, también añade capas de complejidad a la comprensión longitudinal de la interacción entre la protección de datos y los derechos digitales. La necesidad de adaptarse a estos cambios legales subraya la importancia de mantener actualizados los enfoques de investigación y la flexibilidad metodológica para abordar la siempre cambiante realidad jurídica en la protección de datos.

Un tercer aspecto fue que la exploración del terreno de la investigación en este ámbito se ha visto frecuentemente restringida por la ardua dificultad de obtener acceso a información de carácter sensible o clasificada, particularmente

cuando dicha investigación implica la participación de entidades gubernamentales o empresas del sector privado. Este desafío inherente ha planteado obstáculos significativos a la obtención de datos cruciales para comprender y evaluar aspectos relacionados con la seguridad de la información. La restricción de acceso a información delicada ha sido una constante limitación que ha marcado la trayectoria de numerosos estudios en este campo, obstaculizando la capacidad de los investigadores para profundizar de manera exhaustiva en cuestiones vinculadas a la protección de datos en entornos gubernamentales y corporativos. Esta dificultad encuentra su raíz en la naturaleza confidencial y estratégica de la información asociada a la seguridad de datos, que a menudo involucra procesos, tecnologías y políticas sensibles que las entidades gubernamentales y las empresas privadas no están dispuestas a divulgar fácilmente. La reticencia a compartir información clasificada deriva de la necesidad de resguardar la integridad y la confidencialidad de los sistemas y datos críticos para sus operaciones. Esta reticencia crea una barrera significativa para los investigadores que buscan analizar y comprender de manera completa las prácticas, protocolos y eventuales vulnerabilidades en materia de seguridad de datos en estos contextos particulares.

La cuarta limitación identificada en el estudio se encuentra vinculada a la intrincada naturaleza técnica inherente a la seguridad de datos, acentuada por el entorno tecnológico en constante cambio. La rápida evolución de la tecnología exacerbó la complejidad de comprender y evaluar los aspectos técnicos relacionados con la protección de datos y la ciberseguridad. En este escenario dinámico, la dificultad para mantenerse al día con las innovaciones tecnológicas

se convirtió en un desafío significativo, afectando la capacidad de comprender plenamente los mecanismos técnicos que respaldan la salvaguarda de los datos. La constante transformación del entorno tecnológico introduce capas adicionales de dificultad, imponiendo barreras a la aprehensión exhaustiva de las dimensiones técnicas de la protección de datos y la ciberseguridad.

Por otro lado, se vislumbraron desafíos sustanciales en la cooperación internacional cuando se trata de la protección de datos que trascienden las fronteras. Estas dificultades imponen limitaciones significativas, restringiendo la efectividad de la aplicación de la legislación en un contexto global. La complejidad inherente a la gestión de datos a nivel internacional se convierte en un obstáculo que afecta la capacidad de garantizar un cumplimiento uniforme y coherente de las leyes de protección de datos en diferentes partes del mundo.

La dinámica transfronteriza de los datos personales, impulsada por la conectividad global, plantea interrogantes cruciales sobre cómo las jurisdicciones pueden colaborar de manera efectiva. Los límites en la cooperación internacional generan brechas en la capacidad de las autoridades para abordar violaciones potenciales o mal uso de datos que trascienden las fronteras nacionales. Esto, a su vez, debilita la aplicación efectiva de las leyes de protección de datos, ya que la respuesta a los incidentes transfronterizos se ve obstaculizada por la falta de mecanismos y acuerdos robustos de cooperación internacional.

Esta limitación se traduce en una vulnerabilidad inherente en la salvaguarda de los derechos digitales a nivel mundial. La protección de la

privacidad y la integridad de los datos, en un mundo cada vez más interconectado, depende en gran medida de la capacidad de las naciones para colaborar de manera fluida tal como lo señala el Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981. La falta de una cooperación eficiente resalta la necesidad crítica de desarrollar estructuras y protocolos internacionales más sólidos que faciliten una respuesta colectiva y eficaz frente a los desafíos que plantea la protección de datos en el escenario global.

La presencia de expertos en protección de datos y tecnología de la información para brindar asesoramiento o participar activamente en la investigación se vio restringida. Esta restricción plantea un desafío sustancial, ya que la disponibilidad de conocimientos especializados en estas áreas específicas es crucial para la comprensión profunda y precisa de los temas relacionados con la protección de datos. La ausencia de expertos limitó la amplitud y la profundidad con la que se pudo abordar la investigación, ya que estos profesionales desempeñan un papel fundamental en la interpretación de regulaciones complejas, la evaluación de prácticas tecnológicas y la identificación de soluciones eficaces en el ámbito de la protección de datos. La falta de participación de expertos en esta investigación podría haber dejado sin explorar ciertos aspectos clave, como la interpretación detallada de regulaciones específicas o la implementación efectiva de medidas de protección de datos. Este escenario subraya la necesidad de considerar estrategias alternativas para obtener la orientación especializada necesaria, así como la importancia de fomentar la colaboración entre profesionales de la protección de datos y aquellos

involucrados en la investigación para abordar de manera más integral las complejidades de la intersección entre la tecnología y la privacidad.

En el curso de esta investigación, se reveló un componente esencial que no podía ser ignorado: la intrincada red de cuestiones éticas y de privacidad. Este aspecto crítico no solo añadió complejidad a los estudios, sino que también demandó una atención meticulosa a las consideraciones éticas y legales asociadas con la privacidad individual. En este contexto, esta investigación tuvo que abordar de manera meticulosa las profundas implicaciones éticas que surgen al explorar la intersección entre datos personales y derechos digitales. La salvaguardia de la privacidad se convirtió en un principio rector, con cada investigación actuando como un elemento que determina no solo los avances y desafíos en la protección de datos, sino también las responsabilidades éticas intrínsecas a la investigación misma. El respeto riguroso por las leyes y regulaciones en este ámbito no solo fue una prioridad, sino que también se erigió como un pilar fundamental para asegurar que los derechos individuales fueran resguardados con integridad y que los hallazgos resultantes fueran obtenidos de manera ética y legal.

En última instancia, se evidenció una diversidad significativa en las percepciones y el entendimiento general del público en relación con la trascendencia de la protección de datos y los derechos digitales. Estas diferencias notables desempeñaron un papel crucial en la disposición de las personas para involucrarse en esta investigación o para compartir información personal. La gama variada de perspectivas y grados de conocimiento contribuyó a crear un panorama complejo en el que algunos individuos, conscientes y

preocupados por la importancia de salvaguardar sus datos en el entorno digital, mostraron una mayor disposición a participar en este estudio. En contraste, aquellos con percepciones menos claras o conocimientos limitados sobre los riesgos asociados a la privacidad en línea pudieron ser más cautelosos o reacios a compartir información sensible. Esta disparidad en la conciencia y actitudes del público destaca la necesidad no solo de fortalecer la legislación y las políticas de protección de datos, sino también de implementar iniciativas educativas destinadas a mejorar la comprensión general de los derechos digitales. Al abordar estas diferencias de percepción, se puede fomentar una participación más informada y activa en la protección de datos, contribuyendo así a la construcción de un entorno digital más seguro y respetuoso de los derechos individuales en un mundo cada vez más interconectado.

Abordando de manera integral se emprendió una aproximación comprensiva para detallar las limitaciones identificadas en la investigación. Esto conllevó a la realización de un análisis exhaustivo y realista de la protección de datos y los derechos digitales en el marco legal peruano. Este enfoque, minucioso en su naturaleza, no solo buscó entender las disposiciones normativas, sino que también se sumergió en la aplicación práctica de estas leyes en el contexto peruano. En este proceso analítico, se otorgó una atención especial a las consideraciones éticas y legales que subyacen en la investigación sobre temas sensibles como la privacidad de las personas. Se reconoció la necesidad imperante de manejar estos temas con un enfoque ético riguroso, respetando la integridad y derechos de los individuos involucrados. Además, se aseguró que cada fase del proceso de recopilación y análisis de datos estuviera

alineada con los principios legales vigentes, garantizando así la validez y ética de la investigación.

Este análisis profundo no solo se limitó a evaluar la legislación desde un punto de vista teórico, sino que también se sumergió en la realidad práctica de cómo se implementan estas leyes en la dinámica sociedad peruana. Se reconoció que, para obtener una comprensión completa, era esencial considerar tanto el marco legal como su aplicación concreta, identificando posibles brechas y desafíos que podrían impactar la efectividad de la protección de datos y los derechos digitales en el país.

II. REVISION DE LITERATURA

II.1. Marco Teórico

En el ámbito peruano e internacional, la protección de datos también reconocida como “Habeas Data” se erige como un componente fundamental de los derechos fundamentales, proporcionando a los individuos control sobre sus datos personales en un entorno digital en constante evolución. La convergencia de principios y la adaptación a estándares internacionales señalan un reconocimiento global de la importancia de proteger la privacidad y la autodeterminación informativa

Tal es el caso que la protección de datos en la Constitución Política del Perú de 1993 se fundamenta en el reconocimiento de ciertos derechos cuya finalidad es salvaguardar la privacidad y el control sobre la información personal de los ciudadanos. El Artículo 2, Inciso 6 de nuestra Carta Magna establece explícitamente el derecho a la intimidad personal y familiar, así como la inviolabilidad y secreto de la correspondencia y documentos privados. La inclusión del término "habeas data" se relaciona con la protección de la información personal y la facultad de cada individuo para ejercer un control directo sobre sus datos.

Es así que la referencia a la "inviolabilidad" y "secreto" subraya la importancia de resguardar la información personal contra interferencias indebidas y revelaciones no autorizadas. Este contexto refleja la intención de garantizar que los ciudadanos no solo tengan la capacidad de limitar el acceso a sus datos, sino también de mantener su confidencialidad.

Al reconocer el habeas data como un derecho fundamental autónomo, la Constitución reconoce que la protección de la información personal va más allá de simplemente un aspecto secundario de otros derechos. Este reconocimiento como derecho independiente fortalece la posición del ciudadano para controlar y gestionar la información que le concierne directamente. Por ello la amplitud del habeas data en la Constitución Peruana de 1993 les confiere a los ciudadanos una serie de prerrogativas para ejercer control sobre sus datos personales. El reconocimiento como un derecho fundamental autónomo implica que los ciudadanos tienen el derecho de controlar, manejar y decidir sobre la información que concierne a su persona. Esto va más allá de simplemente un derecho de acceso; es la capacidad de determinar quién puede acceder, procesar y utilizar la información personal.

La inclusión en el artículo que garantiza el derecho a la intimidad personal y familiar establece que el habeas data no se trata solo de la protección de datos en sentido estricto, sino que se extiende a la preservación de la esfera íntima y familiar de los individuos. También se debe indicar la importancia de la limitación de interferencias en su tratamiento. Este reconocimiento no solo permite el ejercicio de derechos de manera positiva es decir al acceso a la información; sino también de manera negativa, impidiendo interferencias no autorizadas. Esto refleja un equilibrio entre el derecho de acceso a la información y la protección contra posibles abusos.

La inclusión del habeas data en la Constitución no solo confiere derechos a nivel individual sino que tiene un impacto más amplio en la sociedad al fomentar la protección de la privacidad y la transparencia en el manejo de

información personal. La Constitución Política del Perú de 1993 establece un sólido fundamento para el habeas data, no solo como un derecho fundamental autónomo sino también como una herramienta para empoderar a los ciudadanos en el control y protección de su información personal en concordancia con los principios de intimidad y secreto consagrados en la misma.

Por otro lado la Ley de Protección de Datos Personales en Perú, Ley N° 29733, vigente desde el año 2011, destaca por su enfoque específico en el habeas data y su regulación detallada. Esto debido a que va más allá de simplemente reconocer el habeas data como un principio general. Desarrolla y detalla los principios fundamentales para el tratamiento de datos personales. Esto implica establecer condiciones y límites claros para las entidades que recopilan, almacenan o procesan información personal.

En este sentido la indicada ley establece condiciones específicas que las entidades deben cumplir al tratar datos personales. Esto incluye requisitos de seguridad, procedimientos para obtener el consentimiento del titular y normativas para la transferencia de datos a terceros, entre otros aspectos. El objetivo es garantizar un tratamiento adecuado y ético de la información personal. Por ello esta regulación refleja un compromiso con la protección de la privacidad. La atención especial a los principios de habeas data sugiere una preocupación por el respeto a la intimidad y la autodeterminación informativa de los individuos.

La indicada ley derechos específicos al titular de los datos personales, reconociendo la importancia de empoderar a los individuos en el manejo de su información personal en conceptos tales como el de conocer la información recopilada, actualizar y rectificar información y oponerse al tratamiento.

Puntualizando al respecto, el titular tiene el derecho fundamental de conocer qué información se ha recopilado sobre él. Este derecho a la transparencia es esencial para garantizar que las personas estén al tanto de cómo se están utilizando sus datos. Asimismo la ley reconoce la posibilidad de que la información almacenada pueda volverse obsoleta o incorrecta. Por lo tanto, se otorga al titular el derecho a actualizar y rectificar su información. Esto contribuye a mantener la exactitud de los datos personales. Por otro lado un aspecto crucial es el derecho del titular a oponerse al tratamiento de sus datos personales en ciertas circunstancias. Este derecho respalda la autonomía del individuo, permitiéndole tomar decisiones informadas sobre el uso de su información personal.

Los señalado precedentemente contribuye a promover prácticas éticas en el manejo de datos personales. Esto es esencial para garantizar la confianza de los ciudadanos en la gestión de su información personal. También al reconocer derechos como el acceso y la rectificación, la ley busca empoderar al titular de los datos, cambiando la dinámica de poder hacia el individuo en un entorno en el que la información personal es cada vez más valiosa. Todo esto da lugar a la adaptación constante respecto a los cambios tecnológicos. Su desarrollo específico permite una aplicación efectiva incluso en un contexto digital en constante evolución.

También es materia de análisis la Ley 27489, también conocida como la Ley que regula las centrales privadas de información de riesgo y de protección al titular de la información. Esta norma aborda de forma específica la gestión de información financiera y crediticia por parte de entidades privadas. La ley tiene

como objetivo fundamental regular la creación y funcionamiento de las centrales privadas de información de riesgo. Estas entidades manejan información crediticia y financiera con el propósito de evaluar el riesgo crediticio de los titulares de información.

Uno de los principales enfoques de la ley es garantizar la protección de los derechos de los titulares de la información. Establece medidas específicas para asegurar que la recopilación, almacenamiento y uso de datos financieros se realice de manera justa, transparente y respetando la privacidad de los individuos. La normativa establece los procedimientos y requisitos para que los titulares de información accedan a sus datos almacenados en estas centrales. Este acceso es esencial para que las personas puedan verificar la precisión de la información que se mantiene sobre ellas. La ley destaca la importancia del consentimiento del titular de la información para recopilar y procesar datos. Establece condiciones claras para obtener y registrar este consentimiento de manera que sea informado y libre.

Se establecen disposiciones para garantizar la seguridad de la información manejada por estas centrales. Esto incluye medidas para prevenir accesos no autorizados y garantizar la confidencialidad e integridad de los datos. La legislación exige que estas centrales proporcionen un informe de endeudamiento a los titulares de la información. Este informe es crucial para que las personas conozcan su situación crediticia y tomen decisiones informadas.

Uno de los desafíos es encontrar el equilibrio adecuado entre la protección de la privacidad y el acceso necesario a la información crediticia. Es esencial garantizar que la normativa no obstaculice la operatividad del sistema

crediticio. La efectividad de la ley depende en gran medida de la supervisión y el cumplimiento por parte de las entidades reguladas. Es crucial que existan mecanismos sólidos establecidos para garantizar el acatamiento de las disposiciones señaladas en la ley. Dado el entorno en constante cambio de la tecnología, la ley debe adaptarse para abordar nuevos desafíos y riesgos asociados con el manejo de datos financieros en plataformas digitales.

En el ámbito internacional el Reglamento General de Protección de Datos de la Unión Europea en vigencia desde el año 2016, es una legislación integral que establece estándares rigurosos para la protección de datos y la privacidad de los ciudadanos en la región europea. Este Reglamento se aplica no solo a las entidades establecidas en la Unión Europea sino también a aquellas que ofrezcan bienes o servicios a residentes de la UE o monitoreen su comportamiento. Esto garantiza una protección uniforme y elevada en toda la región. Este reglamento establece los principios rectores fundamentales como la limitación del propósito, la minimización de datos y la exactitud de la información, proporcionando un marco sólido para el manejo ético de los datos personales.

Uno de los ejes de su implementación es que introduce estándares exigentes para la obtención de consentimiento, exigiendo que sea específico, informado y otorgado libremente. Los individuos deben tener control total sobre cómo se utilizan sus datos personales. Por ello reconoce de manera explícita los derechos del titular, muchos de los cuales son análogos al concepto de habeas data. Esto incluye el derecho de acceso para confirmar el procesamiento de datos, rectificación de información incorrecta, supresión de datos irrelevantes y la portabilidad de datos.

Se enfatiza el concepto de “consentimiento activo”, por el cual las organizaciones deben poder demostrar que se obtuvo el consentimiento de manera clara, y los individuos tienen el derecho de retirar su consentimiento en cualquier momento. Asimismo, se requiere que las organizaciones proporcionen información clara y comprensible sobre cómo se procesan los datos personales, garantizando la transparencia en todas las etapas.

Introduce el principio de responsabilidad, donde las organizaciones deben demostrar cumplimiento activo con los principios de protección de datos y poder rendir cuentas por su conformidad. Por ello también establece la obligación de notificar a las autoridades de supervisión y a los individuos sobre violaciones de seguridad de datos en un plazo determinado, asegurando una respuesta rápida y adecuada a las violaciones. Este reglamento introduce sanciones significativas por incumplimiento, que pueden llegar hasta el 4% del volumen de negocios global anual de la empresa infractora. Esto motiva a las organizaciones a implementar medidas de protección de datos sólidas.

También se debe tomar en consideración La Convención 108 del Consejo de Europa del año 1981 es un instrumento clave en el ámbito internacional que establece principios y normas fundamentales para la protección de los derechos individuales en relación con el tratamiento automatizado de datos personales. Este Convención establece un marco sólido para la protección de datos personales. Define estándares que los estados signatarios deben seguir para garantizar que el tratamiento de datos respete los derechos fundamentales de los individuos.

Pone un fuerte énfasis en los derechos individuales en relación con sus datos personales. Esto incluye el derecho a conocer qué información se está recopilando, el propósito de la recopilación y el derecho a rectificar datos inexactos. También destaca la importancia del consentimiento informado. Los individuos deben ser informados de manera clara y comprensible sobre cómo se utilizarán sus datos y deben otorgar su consentimiento de manera libre y específica. Establece que los datos personales deben ser relevantes, adecuados y no excesivos en relación con los fines para los cuales se recopilan y procesan. Asimismo, resalta la necesidad de implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso no autorizado, la divulgación y la destrucción.

Uno de los aspectos más notables de la Convención 108 es su enfoque en la cooperación internacional. Reconoce que la protección efectiva de los datos personales no puede limitarse a las fronteras nacionales y promueve la cooperación entre estados para abordar los desafíos transfronterizos asociados con el tratamiento de datos. Por ello facilita el flujo seguro de datos personales entre los estados miembros al establecer estándares comunes. Esto es esencial en un mundo cada vez más interconectado digitalmente, donde los datos pueden transferirse fácilmente a través de fronteras.

Otro elemento clave es el reconocimiento expreso que los individuos deben gozar de protección incluso cuando sus datos se transfieren a otros países. Esto es crucial en un entorno global donde las empresas y organizaciones operan en múltiples jurisdicciones. La Convención 108 se enfrenta al desafío constante de adaptarse a los cambios tecnológicos. La rápida

evolución de la tecnología digital requiere revisiones periódicas para garantizar que los principios fundamentales sigan siendo efectivos. Una de las dificultades en un contexto global, es que existe la necesidad de armonizar la Convención con otras legislaciones de protección de datos, como el Reglamento General de Protección de Datos de la Unión Europea o la Ley Orgánica 3/2018 de España, entre otras, para garantizar una protección coherente a nivel internacional.

Ley de Privacidad del Consumidor de California, EE. UU, el año 2018, también conocida como CCPA (California Consumer Privacy Act) es una legislación pionera en los Estados Unidos que aborda la privacidad de los consumidores y establece una serie de derechos y responsabilidades clave.

Respecto a los consumidores les da el derecho a saber qué información personal se está recopilando sobre ellos. Las empresas deben revelar qué categorías y tipos de datos se recopilan y con qué fines se utilizan. Uno de los aspectos destacados es el derecho de los consumidores a optar por no participar en la venta de su información personal. Las empresas deben proporcionar un mecanismo claro para que los consumidores ejerzan este derecho. Por otro lado los consumidores tienen el derecho de solicitar la eliminación de sus datos personales de los registros de una empresa. Esto es especialmente relevante cuando los datos ya no son necesarios para los fines para los que fueron recopilados. Esta norma prohíbe la discriminación contra los consumidores que ejercen sus derechos de privacidad. Las empresas no pueden negar servicios, cobrar precios diferentes o proporcionar una calidad inferior basada en el ejercicio de estos derechos.

Respecto a las empresas, estas deben ser transparentes acerca de qué datos están recopilando y con qué propósito. Esto implica la divulgación clara de prácticas de recopilación y uso de datos. La ley exige un enfoque especial para la protección de datos sensibles, como información relacionada con menores de edad. Se requiere un consentimiento explícito para recopilar y procesar dicha información. Por ende las empresas están obligadas a mantener políticas de privacidad claras y accesibles para los consumidores. Estas políticas deben detallar cómo se recopilan, procesan y comparten los datos personales. Esta Ley impone a las empresas la obligación de implementar programas de cumplimiento efectivos. Esto implica no solo cumplir con los derechos del consumidor, sino también establecer prácticas internas que garanticen la seguridad y privacidad de los datos.

Cabe indicar que la implementación de esta norma en EEUU ha resultado desafiante para muchas empresas, especialmente para aquellas que operan a nivel nacional o internacional. Cumplir con los requisitos puede implicar ajustes significativos en las prácticas de manejo de datos. Esto en gran parte a que esta ley es una de las primeras leyes de privacidad de este tipo en los EE. UU. Su evolución y las posibles enmiendas son aspectos por seguir, ya que pueden tener implicaciones significativas en la forma en que las empresas gestionan la privacidad. Por otro lado en un entorno altamente interconectado a nivel transaccional esta ley ha influido en conversaciones más amplias sobre la privacidad y ha inspirado esfuerzos legislativos similares en otros estados y países. Su impacto va más allá de las fronteras de California. Por ello representa un cambio significativo en la forma en que se aborda la privacidad del consumidor en los EEUU. Al otorgar a los consumidores más control sobre sus

datos y establecer responsabilidades claras para las empresas; además sienta un precedente importante para la protección de la privacidad en el entorno digital. Su aplicación y posibles desarrollos futuros son aspectos fundamentales por seguir en el ámbito de la legislación de privacidad.

Mención aparte merece la Ley Orgánica 3/2018, de 5 de diciembre del 2018, que refiere a la Protección de Datos Personales y garantía de los derechos digitales, la misma que pertenece a la legislación española y que aborda temas cruciales relacionados con la protección de datos y los derechos digitales. Esta ley refuerza y actualiza las disposiciones relativas a la protección de datos personales. Establece principios fundamentales, como el consentimiento informado, la minimización de datos y la garantía de la seguridad de la información; aspectos que están en el marco establecido a nivel internacional.

Uno de los aspectos más destacados es la inclusión de garantías específicas para los derechos digitales de los ciudadanos. Esto abarca derechos como la neutralidad de la red, la intimidad en el ámbito digital, la protección contra el spam, y otros aspectos vinculados a la era digital. Otro aspecto es que esta norma establece la obligación para determinadas entidades de designar un “delegado de Protección de Datos”, una figura clave en el cumplimiento de las regulaciones y la gestión de la privacidad.

La ley refuerza el derecho al olvido digital, permitiendo a los individuos solicitar la eliminación de información personal en determinadas circunstancias, especialmente cuando ya no sea relevante o esté desactualizada. También establece normas específicas para el tratamiento de datos personales en el ámbito laboral, protegiendo la privacidad de los empleados y fijando límites

claros para la monitorización de actividades laborales. Asimismo la normativa presta especial atención a la protección de los derechos digitales de los menores, introduciendo salvaguardias específicas para el tratamiento de sus datos en entornos digitales. Por último resalta la obligación de obligación de mantener un registro de actividades de tratamiento, proporcionando una mayor transparencia sobre cómo se están utilizando los datos personales.

La Ley Orgánica 3/2018 es compatible con el Reglamento General de Protección de Datos de la Unión Europea. Esta alineación fortalece la posición de España en el contexto internacional y facilita la transferencia segura de datos con otras jurisdicciones. La legislación tiene un impacto significativo en la forma en que empresas y organizaciones manejan los datos personales. Requiere una revisión y ajuste de políticas internas para cumplir con los nuevos requisitos. Por ello la ley adopta un enfoque proactivo hacia la protección de derechos digitales, reconociendo la importancia de adaptarse a los desafíos emergentes en la era digital.

II.2. Antecedentes del estudio

En los antecedentes nacionales podemos encontrar a Salinas & Vasquez (2023), cuyo objetivo central fue analizar el nivel de cumplimiento de la ley de protección de datos personales en una entidad privada de salud en Perú. El investigador buscó evaluar cómo se maneja y protege la información personal dentro de esta organización, determinando si hay un cumplimiento adecuado de la legislación pertinente. La investigación se clasificó como descriptiva, ya que se enfocó en proporcionar una descripción detallada y específica de la situación actual respecto al cumplimiento de la ley de protección de datos personales en la

entidad de salud. Se seleccionaron y analizaron elementos específicos de la ley, centrándose en los Títulos III y IV, con el propósito de realizar una evaluación detallada y específica. Los resultados revelaron un conflicto entre el derecho a la protección de datos personales y el derecho a la intimidad en el contexto de una entidad privada de salud en Perú. A pesar de la existencia de la Ley N° 29733 que regula la protección de datos personales en el país, la entidad presentó un cumplimiento del 65%, indicando un incumplimiento del 35% de los lineamientos establecidos por la legislación. La falta de cumplimiento se atribuyó al desconocimiento o mala aplicación de la ley dentro de la organización, evidenciando una brecha entre las políticas y reglamentos internos de la entidad y los requisitos establecidos por la ley de protección de datos personales. En consecuencia, se propuso una serie de alternativas destinadas a fortalecer la ley y mejorar la implementación y el cumplimiento de la normativa dentro de la entidad de salud. La investigación es crucial en el contexto de la protección de datos y derechos digitales, ya que destaca las deficiencias en la aplicación de la legislación existente en el ámbito privado de la salud. Proporciona una visión detallada de cómo las entidades manejan la información personal y revela la necesidad de un mayor cumplimiento y alineación con las leyes de protección de datos. La propuesta generada como resultado de la investigación busca no solo corregir las deficiencias identificadas sino también establecer un proceso de mejora continua. Esto beneficia no solo a la entidad en cuestión sino que también establece un precedente para otras organizaciones, contribuyendo así a la protección efectiva de los datos personales y la promoción de los derechos digitales en el ámbito de la salud en el Perú.

Huerta & Cochachin (2021), en su investigación, se propusieron analizar y comprender por qué el derecho al olvido digital puede considerarse una solución viable para resolver el conflicto entre la libertad de información y el derecho a la protección de datos personales en el contexto peruano. La exploración se centró en cómo este derecho puede aplicarse y cuáles son sus implicaciones, prestando especial atención a la normativa, jurisprudencia y doctrina relevantes en el país. La investigación adoptó un enfoque dogmático, fundamental para el análisis de cuestiones legales, y se clasificó como no experimental. No implicó la manipulación de variables en un entorno controlado, sino más bien la observación y análisis de documentos legales, casos judiciales y discusiones doctrinales. Además, se caracterizó como transversal y descriptiva, abordando el tema en un momento específico y buscando describir y comprender la situación legal y jurisprudencial actual en relación con el derecho al olvido digital en Perú. Los hallazgos concluyeron que el derecho al olvido digital se refiere al derecho de impedir la difusión de información personal en internet cuando la publicación no cumple con los requisitos de adecuación y pertinencia establecidos por la normativa legal. Específicamente, se reconoció el derecho a limitar la difusión universal e indiscriminada de datos personales en motores de búsqueda generales, especialmente cuando la información es obsoleta o ya no posee relevancia o interés público. Se subrayó que este derecho puede aplicarse incluso en situaciones donde la publicación original fue legítima, como en el caso de información en boletines oficiales o protegida por las libertades de expresión o información. La investigación resaltó la importancia del derecho al olvido como una herramienta legal crucial para equilibrar la libertad de información con la protección de datos personales. Al evidenciar que

el almacenamiento ilimitado de información personal en línea puede atentar contra la privacidad y el derecho a la protección de datos, la investigación abogó por la implementación de medidas que limiten la perennidad de la información en línea. Esto no solo resguarda la intimidad de las personas, sino que también reconoce la evolución de la relevancia e interés público de ciertos datos con el tiempo. En última instancia, la investigación aboga por el reconocimiento y aplicación del derecho al olvido como una herramienta esencial para proteger los derechos digitales y la privacidad en el entorno digital peruano.

Luna Cervantes (2021), en su investigación, se propuso brindar una visión informativa y reflexiva sobre la protección de datos personales en el contexto peruano, con un enfoque en el período que abarca el final de la década actual. La intención principal fue explorar y abordar las cuestiones clave relacionadas con la protección de datos en Perú, aprovechando tanto la experiencia práctica en la Autoridad Nacional de Protección de Datos Personales como las reflexiones académicas derivadas de esta función. Esta investigación se caracteriza como un análisis informativo y reflexivo, basado en una libre asociación de ideas presentadas en formato de preguntas y respuestas, sugiriendo un enfoque cualitativo. Además, se destaca que parte de la información proviene de la experiencia práctica en la Autoridad Nacional de Protección de Datos Personales y de la reflexión académica, indicando una investigación basada en la práctica y en la revisión crítica de literatura y políticas relacionadas con la protección de datos. Las conclusiones extraídas de esta investigación resaltan las dinámicas y desafíos específicos relacionados con la protección de datos en el contexto peruano al final de la década. Se abordan aspectos como la eficacia de las políticas existentes, las tendencias emergentes,

las áreas de mejora y las consideraciones éticas en juego. Estas conclusiones se fundamentaron en la experiencia práctica y en el análisis académico, proporcionando una visión integral de la situación actual de la protección de datos en Perú. La relevancia de esta investigación radica en su capacidad para arrojar luz sobre la situación específica de la protección de datos personales en Perú al final de la década. Proporciona una oportunidad para evaluar la eficacia de las políticas y prácticas existentes, identificar áreas de mejora y destacar desafíos emergentes. Además, al fusionar la experiencia práctica con la reflexión académica, la investigación ofrece perspectivas valiosas que contribuyen al desarrollo y la implementación efectiva de políticas futuras en materia de protección de datos y derechos digitales en el país.

Revoredo-Palacios (2021), en su investigación cuyo objetivo fundamental fue explorar en profundidad el concepto emergente de publicidad programática, con un enfoque particular en su relación con el uso de datos personales. La investigación buscó arrojar luz sobre los elementos clave que definían la publicidad programática, examinar cómo esta práctica mejoraba la entrega de contenido publicitario en un entorno digital, y, crucialmente, evaluar el uso de datos personales en este contexto. Además, realizó una comparativa detallada de la legislación aplicable en el Perú y en la Unión Europea para comprender cómo cada jurisdicción abordaba la protección de datos en el ámbito de la publicidad programática. Esta investigación adoptó un enfoque mixto que incluyó tanto métodos cualitativos como cuantitativos. Se llevó a cabo un análisis exhaustivo de la literatura existente para comprender las tendencias y prácticas actuales en la publicidad programática. Además, se llevaron a cabo entrevistas y encuestas con expertos en la materia y profesionales de la industria publicitaria

para obtener perspectivas prácticas y experiencias sobre el uso de datos personales en la publicidad programática. Este enfoque mixto permitió una comprensión holística del tema desde múltiples perspectivas. Las conclusiones fundamentales sobre la intersección entre la publicidad programática y la protección de datos personales incluyeron hallazgos sobre las prácticas actuales de recopilación y uso de datos personales en la publicidad programática, así como una evaluación de la efectividad de las leyes en vigor en el Perú y en la Unión Europea para salvaguardar los derechos de privacidad en este contexto. Se señalaron en las conclusiones posibles brechas en la protección de datos y se plantearon recomendaciones para mejorar la regulación o las prácticas empresariales en este ámbito. Esta investigación fue crucial en el contexto actual de rápido avance tecnológico y creciente preocupación por la privacidad en línea. La publicidad programática, al depender en gran medida del uso de datos personales, presentó desafíos significativos en términos de protección de la privacidad. Comprender cómo se abordaba este desafío en jurisdicciones específicas como el Perú y la Unión Europea fue esencial para garantizar una protección efectiva de los derechos digitales. Los hallazgos de esta investigación no solo informaron a las autoridades reguladoras y legisladores, sino que también proporcionaron orientación valiosa para las empresas que participan en la publicidad programática, ayudándolas a alinear sus prácticas con los estándares éticos y legales más altos. En última instancia, la investigación contribuyó al desarrollo de políticas y prácticas que equilibraron eficazmente la innovación en publicidad digital con la necesidad crítica de proteger la privacidad de los usuarios.

Saavedra-Grados (2023), en su investigación, que tuvo como objetivo general analizar si la regulación jurídica de la ley de protección de datos personales vulnera la intimidad de las personas en Tarapoto durante el periodo 2020-2022. La investigación adoptó un enfoque cualitativo, buscando una comprensión profunda y detallada del fenómeno estudiado. Se clasificó como investigación básica, orientada a obtener una comprensión teórica y conceptual del problema, utilizando un diseño de estudio de casos para profundizar en el contexto específico de Tarapoto. Los hallazgos de la investigación revelaron que existe una significativa vulneración del uso de datos personales, especialmente por parte de empresas privadas en la región de Tarapoto durante el periodo estudiado. Esta vulneración compromete la privacidad de los individuos en la región. Además, a pesar de la existencia de la Ley N° 29733, se concluyó que hay un incumplimiento generalizado de esta disposición legal por parte de las empresas, evidenciando un desconocimiento o ignorancia de las regulaciones establecidas para proteger los datos personales. En cuanto al impacto negativo significativo, se destacó que la vulneración de datos tiene un impacto negativo importante, especialmente en el derecho a la protección de datos personales. Esto subraya la necesidad de abordar la debilidad en la aplicación de la ley para garantizar la protección de la privacidad. La investigación también señaló una debilidad en los órganos competentes encargados de hacer cumplir la ley, lo que contribuye a la falta de aplicación efectiva de las disposiciones legales existentes y permite la vulneración de datos. La investigación es crucial para la generación de conocimiento sobre la situación específica en Tarapoto, proporcionando una visión detallada de cómo la regulación legal impacta la protección de datos. Además, alerta sobre vulnerabilidades existentes en la región, destaca la

necesidad de intervenciones legislativas y ofrece información valiosa para mejorar las leyes y fortalecer la protección de datos personales. También puede servir como una herramienta para crear conciencia en la sociedad y entre las empresas sobre la importancia de respetar la privacidad y cumplir con las leyes de protección de datos. En resumen, la investigación no solo identifica problemas específicos en la protección de datos en Tarapoto, sino que también destaca la necesidad de intervenciones efectivas para garantizar una aplicación adecuada de las leyes y proteger los derechos digitales de los individuos.

Rudas y Carpio (2022), en su investigación cuyo objetivo principal fue analizar la afectación al derecho a la privacidad de los usuarios del Banco de Crédito debido al tratamiento inadecuado de sus datos personales en el año 2021. La investigación adoptó un diseño básico, utilizando un enfoque cualitativo y de nivel descriptivo. La elección de un diseño fenomenológico de casos permitió explorar en profundidad la experiencia de los usuarios en relación con la protección de sus datos personales en el Banco de Crédito. El carácter cualitativo facilitó la comprensión detallada de los fenómenos y la interpretación de las percepciones y experiencias de los participantes. Los resultados de la investigación revelaron una vulneración significativa al derecho a la privacidad de los usuarios del Banco de Crédito debido al inadecuado tratamiento de sus datos personales. Se evidenció un uso incorrecto de la información, infringiendo el principio de finalidad establecido en la Ley Nro. 29733 Ley de Protección de Datos Personales y su Reglamento. Además, se destacó la ausencia de mecanismos efectivos de control que impidieran la filtración de información, contribuyendo así a la transgresión del derecho a la privacidad y a la intimidad personal de los usuarios. Se identificó una subcategoría emergente relacionada

con una mayor difusión de la Ley Nro. 29733 Ley de Protección de Datos Personales, sugiriendo que la investigación ha contribuido a la concientización y conocimiento más amplio sobre la normativa de protección de datos, señalando la necesidad de difundir y promover el cumplimiento de estas normas. La investigación es relevante en el ámbito de la protección de datos y derechos digitales al poner de manifiesto las fallas en el tratamiento de la información personal por parte de una institución financiera importante. Identificar estas deficiencias proporciona insumos valiosos para el diseño de estrategias y políticas que fortalezcan la protección de datos en entornos financieros. Además, al aumentar la conciencia sobre la Ley Nro. 29733, contribuye a la creación de una cultura de respeto a la privacidad digital y fomenta la adopción de prácticas más seguras en el manejo de datos personales.

Con relación a los antecedentes internacionales, Lombarte (2020), en su investigación cuyo propósito fue analizar las estrategias, actores, condiciones y debates relacionados con los derechos digitales en el contexto de la pandemia de COVID-19 en México, Argentina y Brasil. El estudio se propuso examinar cómo los derechos digitales, específicamente el acceso, la privacidad y la libertad de expresión, fueron tratados durante este período crítico, destacando las variaciones en las políticas estatales y las respuestas de diferentes actores involucrados. El tipo de investigación se enmarca en un análisis comparativo teórico-normativo y sociopolítico. Desde un enfoque teórico-normativo, se busca evaluar cómo se han abordado conceptualmente los derechos digitales en el marco de la comunicación como un derecho humano fundamental y las políticas de comunicación. En cuanto al enfoque sociopolítico, la investigación se propone comprender cómo las condiciones políticas, las políticas públicas previas y las

adoptadas específicamente en respuesta a la pandemia, y las dinámicas de poder entre los actores, han influido en las estrategias y debates sobre derechos digitales. Las conclusiones de la investigación reflejan una diversidad de estrategias y enfoques en relación con los derechos digitales en los tres países estudiados. Los debates principales se centraron en el acceso, la privacidad y la libertad de expresión. Se observó que las políticas estatales variaron según la orientación política de los gobernantes, las políticas públicas existentes y las adoptadas en respuesta a la pandemia. Las empresas, por su parte, implementaron estrategias que, en algunos casos, fueron regresivas pero que, ante presiones sociales, se vieron obligadas a revertir. También se destacaron estrategias progresivas, aunque excepcionales. La sociedad civil y los organismos internacionales jugaron un papel crucial al impulsar soluciones progresivas a largo plazo. Esta investigación es importante en el contexto de la protección de datos y derechos digitales, ya que arroja luz sobre cómo estos derechos han sido abordados en situaciones excepcionales, como una pandemia. Proporciona información valiosa sobre las tensiones entre las políticas estatales, las estrategias empresariales y las demandas de la sociedad civil, delineando la complejidad de garantizar derechos digitales en momentos críticos. Estos hallazgos son esenciales para informar futuras políticas y prácticas, resaltando la necesidad de soluciones progresivas y la importancia de la participación ciudadana y la presión internacional en la protección de datos y derechos digitales.

Barrio (2021), en su investigación cuyo objetivo fue explorar el contexto, concepto y desarrollos de los derechos digitales en el año 2021, considerando la positivización actual en la Ley Orgánica 3/2018 de Protección de Datos

Personales y garantía de los derechos digitales en España. Además, se buscó examinar las novedades que se incorporarán en la próxima Carta de Derechos Digitales de España, que se encuentra en la fase final de redacción. El estudio también pretendió analizar los posibles pasos futuros en la evolución de los derechos digitales, incluida la perspectiva de un nuevo orden jurisdiccional adaptado a los procedimientos y tiempos de resolución del entorno digital. La investigación adoptó un enfoque analítico y descriptivo para explorar el contexto actual de los derechos digitales. Se basó en el análisis de la legislación vigente, con un énfasis especial en la Ley Orgánica 3/2018 y las perspectivas futuras que se anticipan con la Carta de Derechos Digitales. Además, se puede considerar como una investigación prospectiva, ya que examina los posibles pasos futuros en la evolución de los derechos digitales y plantea la posibilidad de un nuevo orden jurisdiccional. Las conclusiones de la Investigación destacaron la urgencia de abordar la transición de la era analógica a la digital, señalando la falta de un entorno de seguridad jurídica en esta transformación. Subrayó la importancia crucial de los derechos digitales en este nuevo paradigma, como se refleja en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Por otro lado, anticipó la relevancia de la próxima Carta de Derechos Digitales de España en la consolidación y expansión de estos derechos. La investigación también apuntó hacia la posibilidad de un nuevo orden jurisdiccional adaptado a los asuntos digitales, sugiriendo una evolución significativa en la protección legal en el entorno digital. Remarcó la importancia de la Investigación para la Protección de Datos y Derechos Digitales es crucial para la comprensión y fortalecimiento de los derechos digitales en la sociedad actual. Ofrece una visión clara del marco legal existente y futuro en relación con

la protección de datos y derechos digitales en España. Al explorar las lagunas en la seguridad jurídica durante la transición digital, la investigación destaca la necesidad de adaptar y fortalecer las leyes para garantizar la protección efectiva de los ciudadanos en el entorno digital. La importancia radica en informar y orientar las discusiones y decisiones legislativas hacia un futuro donde los derechos digitales estén sólidamente establecidos y protegidos en la era digital.

Moreno-Bobadilla (2020), en su investigación, cuyo objetivo fue analizar el desarrollo y la evolución del derecho al olvido digital en Europa, se partió desde las primeras sentencias anteriores a la era de Internet hasta llegar al caso clave de 2014, el Caso Costeja. La investigación buscó comprender la génesis y la transformación de este derecho, además de analizar cómo este punto de inflexión influyó directamente en la legislación, tanto a nivel de la Unión Europea como en los ordenamientos jurídicos nacionales de sus Estados miembros. Este estudio adoptó un enfoque histórico y jurídico, repasando cronológicamente las sentencias pre-Internet, centrándose en el Caso Costeja como un momento crucial y analizando la legislación subsiguiente. Se situó en el ámbito jurídico y legal, incorporando una perspectiva histórica para contextualizar y comprender la evolución de este derecho en respuesta a los cambios tecnológicos y sociales. Las conclusiones de la investigación revelaron la complejidad del derecho al olvido digital y su evolución en el contexto europeo. Se demostró cómo este derecho fue moldeado por decisiones judiciales previas a la era digital y cómo el Caso Costeja, al establecer un precedente, impactó directamente en la legislación europea y nacional. Se concluyó que el derecho al olvido digital es un concepto poliédrico, en constante cambio y adaptación, reflejando la complejidad de la sociedad digital actual. La importancia de la investigación para la protección

de datos y derechos digitales radica en que resalta la importancia del derecho al olvido digital como un componente esencial de la protección de datos y derechos digitales en Europa. Al explorar su evolución y su impacto en la legislación, la investigación contribuyó a la comprensión crítica de cómo los marcos legales se adaptan a los desafíos únicos que plantea la era digital. Esto tiene implicaciones significativas para la garantía de la privacidad y la autonomía de los ciudadanos en un entorno digital en constante cambio, marcando pautas importantes para la formulación de políticas y legislación futuras en la protección de datos personales y derechos digitales.

Segura (2019), en su investigación, cuyo objetivo principal fue examinar el papel de los actores progresistas de la sociedad civil en la promoción de políticas públicas basadas en derechos digitales en América Latina, se buscó comprender cómo estos actores influyeron en la formulación de políticas que establecieran límites a los abusos tanto del Estado como del mercado en la esfera de la comunicación pública. Además, se pretendió explorar cómo estas políticas buscaban proteger y garantizar los derechos de los ciudadanos en relación con la comunicación y la cultura en la era digital. Este trabajo se enmarcó como una investigación cualitativa, centrándose en comprender y analizar fenómenos sociales, específicamente el activismo por los derechos digitales en América Latina. Utilizó enfoques cualitativos para explorar las motivaciones, estrategias y desafíos de los movimientos sociales que abogaban por políticas basadas en derechos en el contexto digital y de protección de datos. La investigación destacó la diversidad de actores involucrados en el activismo por los derechos digitales, incluidos movimientos sociales, gobiernos, corporaciones y organizaciones criminales. Se concluyó que esta diversidad

implicaba una complejidad significativa en la formulación de políticas y estrategias. Asimismo, evidenció desafíos específicos en América Latina relacionados con el acceso, producción y gestión digital y de datos. Las conclusiones sugirieron que, si bien había similitudes con los desafíos en países centrales, también existían particularidades regionales que debían abordarse de manera específica. La investigación arrojó luz sobre la discusión sobre si los problemas generados por la tecnología digital eran realmente nuevos o si representaban la repetición de problemas ya existentes. Se concluyó que, en muchos casos, había elementos novedosos, pero también se entrelazaban con problemas históricos. También se identificó que la región estaba inmersa en un proceso de construcción de nuevos marcos interpretativos relacionados con los derechos digitales. Esto implicaba una reevaluación constante de demandas, oponentes, aliados y estrategias por parte de los actores involucrados. La relevancia de esta investigación radicó en su contribución al entendimiento de la dinámica del activismo por los derechos digitales en América Latina. Proporcionó conocimientos valiosos sobre cómo se estaban abordando los retos de la tecnología digital en la región y cómo los actores progresistas de la sociedad civil estaban influyendo en la formulación de políticas públicas. Estos hallazgos fueron esenciales para informar futuras acciones y políticas que buscaban equilibrar la protección de datos y derechos digitales en un contexto regional específico, destacando la importancia de un enfoque contextualizado y adaptado a las realidades latinoamericanas.

Roca (2020), en su investigación cuyo objetivo principal fue analizar el impacto y la evolución del derecho a la protección de datos en el contexto europeo, específicamente bajo el marco del Reglamento General de Protección

de Datos y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, buscó comprender cómo estas regulaciones respondieron y adaptaron el derecho de protección de datos a los avances tecnológicos, con un enfoque particular en el papel del consentimiento del interesado. Esta investigación adoptó un enfoque jurídico y analítico, basándose en el análisis de las disposiciones y sentencias del Tribunal de Justicia de la Unión Europea, del Tribunal Europeo de Derechos Humanos y del Tribunal Constitucional. Además, se llevó a cabo un estudio comparativo entre las corrientes anglosajona y germana del derecho fundamental a la protección de datos. El método empleado implicó una revisión exhaustiva de la legislación pertinente y de la jurisprudencia relevante para identificar la evolución y los posibles puntos débiles en la regulación, especialmente en relación con el consentimiento del interesado. Las conclusiones de la investigación, enmarcadas dentro de la "Evolución Jurisprudencial", constatan que la evolución del derecho a la protección de datos es más notable en las resoluciones del Tribunal Constitucional en comparación con los tribunales europeos. Esto indica una adaptación activa y continua a los cambios tecnológicos por parte de la jurisprudencia nacional. La investigación destaca la importancia del consentimiento del interesado como una pieza clave de la protección de datos. No obstante, identifica posibles puntos débiles en la normativa actual, sugiriendo la necesidad de revisar y fortalecer las disposiciones relacionadas con el consentimiento para abordar las complejidades emergentes. La investigación arroja luz sobre la dinámica entre la legislación europea y nacional en el ámbito de la protección de datos. Además proporciona una comprensión más profunda de cómo los derechos digitales se están adaptando a un entorno digital en

constante cambio. Además, al resaltar posibles debilidades en la regulación actual, la investigación aboga por una mayor atención a la protección del consentimiento del interesado, contribuyendo así a fortalecer las salvaguardas legales en el ámbito de la protección de datos.

Castellanos Claramunt (2020), en su investigación cuyo objetivo principal fue analizar la gestión de la información en la era digital, centrándose en el tratamiento de datos personales a través de la inteligencia artificial. Se buscó comprender la repercusión jurídica y social de este fenómeno, teniendo en cuenta tanto la normativa comunitaria como la española. Además, se pretendió explorar nuevos derechos surgidos de la protección de datos, como el derecho al olvido, y examinar cómo la inteligencia artificial influye en cuestiones políticas, así como en sectores como la educación y la salud. Esta investigación se enmarca en un enfoque multidisciplinario que combina elementos jurídicos y éticos. Utilizó métodos cualitativos para analizar la normativa legal y ética relacionada con la gestión de la información y la inteligencia artificial. También incorporó elementos de análisis social para comprender la incidencia política y las implicaciones en sectores específicos como la educación y la salud. La metodología incluyó revisión bibliográfica, análisis de casos, y entrevistas a expertos en derecho, ética y tecnología. La investigación concluye que la gestión de la información en la era digital no solo es un tema legal, sino que tiene profundas implicaciones éticas y sociales. Se identifican nuevos derechos, como el derecho al olvido, que emergen de la necesidad de proteger los datos personales en un contexto de inteligencia artificial. Se destaca la importancia de considerar tanto aspectos éticos como jurídicos al implementar sistemas de inteligencia artificial para gestionar los derechos y datos personales de los

ciudadanos. Además, se evidencia la relevancia de abordar cuestiones como la automatización de decisiones y el uso de datos en ámbitos críticos como la educación y la salud. La investigación es crucial en el contexto de la protección de datos y derechos digitales, ya que arroja luz sobre las complejidades éticas y jurídicas de la gestión de la información en la era digital. Proporciona “insights” valiosos para legisladores, profesionales del derecho y desarrolladores de tecnología sobre cómo abordar la implementación de la inteligencia artificial de manera ética y legal. Al destacar la interconexión entre la gestión de datos y la protección de derechos fundamentales, la investigación contribuye a la formación de políticas y prácticas que salvaguarden la privacidad y otros derechos en un entorno digital en constante evolución.

Vázquez-Cano & Pascual-Moscoso (2022), en su investigación conjunta cuyo objetivo fue analizar el conocimiento del profesorado en relación con los procedimientos de protección de datos y el uso ético y responsable de la tecnología, en concordancia con los parámetros establecidos por la Unión Europea para un uso sostenible de la tecnología en la educación. Se busca comprender la percepción y la importancia que el profesorado asigna a los procedimientos de protección de datos, derechos de autor, el uso ético y seguro de dispositivos digitales en los procesos de enseñanza-aprendizaje, así como evaluar la relevancia de la formación del profesorado en estas dimensiones. La investigación adopta un enfoque mixto, combinando elementos cuantitativos y cualitativos. Utiliza métodos cuantitativos para evaluar el conocimiento y la importancia que los docentes atribuyen a las cuestiones de protección de datos y ética en el uso de la tecnología. Simultáneamente, emplea métodos cualitativos para obtener una comprensión más profunda de las percepciones y experiencias

del profesorado en relación con estas cuestiones. Esta combinación permite una visión holística y enriquecedora de la problemática estudiada. Los resultados revelan que la formación es una variable determinante para promover una didáctica sostenible en el uso de la tecnología en la educación. La carencia de conocimientos por parte del profesorado en los protocolos y normas de uso de dispositivos y programas informáticos para garantizar la protección de datos y los derechos del menor en entornos digitales es un hallazgo significativo. Además, se identifica la percepción de que el uso poco sostenible de dispositivos digitales puede tener impactos psicoemocionales en los estudiantes. Esto destaca la necesidad de abordar estas preocupaciones de manera integral y transversal en las diferentes áreas de enseñanza para prevenir posibles perjuicios. La investigación subraya la importancia crítica de la formación del profesorado en cuestiones de protección de datos y ética en el uso de la tecnología. Al identificar lagunas en el conocimiento y las prácticas actuales, proporciona una base para desarrollar programas de capacitación específicos. Además, al señalar la percepción del profesorado sobre los posibles perjuicios psicoemocionales asociados con el uso poco sostenible de dispositivos digitales, destaca la necesidad de enfoques pedagógicos que integren prácticas éticas y seguras en la integración de la tecnología en la educación. Esta investigación contribuye a la mejora de las prácticas educativas y la protección de datos en entornos digitales.

II.3. Bases Teóricas

Se ha identificado las siguientes teorías relacionadas a la protección de datos personales e identidad digital: la teoría de la autodeterminación de la

información, privacidad como derecho fundamental, contrato social digital, justicia distributiva de la información, autenticidad e integridad personal, valor instrumental de la privacidad y de la ética de la privacidad. A continuación reseñaremos las teorías identificadas:

La Teoría de la “Autodeterminación de la Información”; es un principio ético y legal que defiende el derecho fundamental de las personas a controlar la información que comparten sobre sí mismas. En esencia esta teoría está la noción de que cada individuo tiene el derecho de tener control sobre su propia información personal. Esto significa que las personas deberían poder decidir qué información desean compartir y cuál prefieren mantener privada. Por ello la teoría aboga por el concepto de consentimiento informado. Esto implica que las personas deben estar plenamente informadas sobre cómo se utilizará su información antes de proporcionarla. El consentimiento debe ser explícito y basarse en un entendimiento claro de las implicaciones.

Por otro lado la recopilación y uso de datos deben limitarse al propósito específico para el cual se obtuvo el consentimiento. Es decir, si una persona proporciona datos para un propósito específico, no se debe utilizar para otros fines sin su consentimiento adicional. La teoría defiende el derecho de las personas a acceder a la información que las organizaciones tienen sobre ellos. Además, deben tener la capacidad de corregir cualquier información inexacta. Esto contribuye a la transparencia y permite que los individuos mantengan el control sobre su representación en las bases de datos. Además esta teoría subraya la importancia de garantizar la seguridad y privacidad de los datos. Las organizaciones que recopilan información deben implementar medidas

adecuadas para protegerla contra el acceso no autorizado y garantizar que se utilice de manera ética. Las personas deberían tener el derecho de retirar su consentimiento en cualquier momento. Esto significa que pueden solicitar que se deje de recopilar o utilizar su información, y las organizaciones deben respetar esa solicitud.

La Teoría de la Autodeterminación de la Información busca empoderar a los individuos. Al darles el control sobre su información, se les reconoce como agentes autónomos capaces de tomar decisiones informadas sobre la gestión de su privacidad. La teoría destaca la importancia de que las organizaciones actúen de manera ética y asuman la responsabilidad de proteger los derechos de privacidad de las personas. Esto implica no solo cumplir con la ley, sino ir más allá para garantizar prácticas éticas y transparentes

La "Teoría de la Privacidad como Derecho Fundamental" aborda la privacidad como un elemento esencial e inherente a la dignidad humana y a los derechos fundamentales de las personas. Esta perspectiva reconoce que la privacidad no es simplemente una conveniencia o un lujo, sino un derecho intrínseco que debe ser respetado y protegido en sí mismo. La teoría parte del principio de que la privacidad es esencial para preservar la dignidad humana. Implica que la capacidad de controlar la información personal y decidir qué compartir con otros es fundamental para el respeto y la integridad de cada individuo.

En esta perspectiva, la protección de datos personales se considera una extensión de los derechos humanos básicos. El derecho a la privacidad se vincula directamente con otros derechos fundamentales, como la libertad de

expresión, la libertad de asociación y el derecho a un juicio justo. La teoría sostiene que la privacidad es esencial para la libertad individual. La capacidad de controlar la propia información permite a las personas tomar decisiones informadas sobre cómo desean vivir sus vidas, interactuar con otros y participar en la sociedad. Esta teoría reconoce que la privacidad es una salvaguarda crucial contra el poder intrusivo del Estado. Limitar el acceso y el uso indebido de la información personal por parte del gobierno es esencial para prevenir abusos de poder y proteger las libertades individuales.

Esta teoría respalda la necesidad de leyes y regulaciones que protejan la privacidad de las personas. La creación de marcos legales que establezcan cómo se deben recopilar, almacenar y utilizar los datos personales es una aplicación práctica de esta teoría. En el ámbito de la investigación y la tecnología, esta teoría aboga por prácticas éticas que respeten la privacidad. Implica que las organizaciones deben diseñar tecnologías y realizar investigaciones de manera que respeten la autonomía y la dignidad de los individuos. También destaca la importancia de garantizar que las personas tengan control sobre su propia información y que tengan acceso a la información que se recopila sobre ellas. Esto implica derechos como el acceso a sus datos personales y la capacidad de corregir información incorrecta. La teoría sugiere que la educación y la concientización sobre la importancia de la privacidad son cruciales. Informar a las personas sobre sus derechos y cómo pueden proteger su privacidad contribuye a fortalecer la comprensión y la defensa de este derecho fundamental.

La Teoría del “Contrato Social Digital” es una perspectiva que aborda la relación entre los individuos y las plataformas en línea desde una óptica

contractual. Esta teoría sugiere que existe un acuerdo implícito entre los usuarios y las plataformas en línea cuando los usuarios proporcionan sus datos personales. Este acuerdo implica que los usuarios están dispuestos a compartir información a cambio de acceder a los servicios y beneficios ofrecidos por la plataforma.

Las plataformas digitales, al recopilar datos, adquieren una responsabilidad ética en virtud de este "contrato". Se espera de ellas que manejen los datos de manera ética, protegiendo la privacidad de los usuarios y utilizando la información de una manera que beneficie a los usuarios en lugar de perjudicarlos. También se establecen principios clave de protección de datos, esto incluye la transparencia en la recopilación y uso de datos, el consentimiento informado de los usuarios, la seguridad robusta para evitar brechas de datos y el acceso y control que los usuarios deben tener sobre sus propios datos.

Esta teoría busca empoderar a los usuarios al reconocer que tienen derechos en esta relación contractual. Esto implica el derecho a conocer cómo se utilizan sus datos, el derecho a negarse a ciertos usos y el derecho a retirar su consentimiento en cualquier momento. La naturaleza del contrato puede cambiar con el tiempo y con las políticas de la plataforma. Por ejemplo, si una plataforma decide cambiar sus prácticas de privacidad, esto podría considerarse una modificación del contrato, y los usuarios podrían evaluar si desean continuar participando. Cuando las plataformas no cumplen con los principios éticos establecidos en este contrato digital, existe el riesgo de violación del acuerdo. Esto podría tener consecuencias legales y también afectar la confianza de los usuarios en la plataforma.

En algunos casos, los aspectos de este "contrato" se traducen en términos legales, como se refleja en las leyes de privacidad y protección de datos. Las legislaciones, como el Reglamento General de Protección de Datos de la Unión Europea, refuerzan y respaldan los principios contractuales entre usuarios y plataformas. Por ende la Teoría del Contrato Social Digital proporciona un marco conceptual útil para entender la dinámica entre los usuarios y las plataformas en línea en el contexto de la recopilación y el uso de datos personales. Destaca la importancia de una relación ética y transparente para mantener la confianza y el equilibrio en esta interacción digital.

La Teoría del "Valor Instrumental de la Privacidad" se centra en el papel crucial que la privacidad juega como un instrumento para lograr otros valores fundamentales en una sociedad, como la libertad, la autonomía y la democracia. Esta perspectiva ve la privacidad como un medio, más que un fin en sí mismo. Por ello destaca la privacidad se la considera esencial para la libertad individual. En un entorno en el que las acciones y la información de las personas pueden ser monitoreadas constantemente, la privacidad actúa como un resguardo que permite a las personas actuar y expresarse sin temor a represalias o juicios indebidos.

Por otro lado la capacidad de tomar decisiones informadas y ejercer el control sobre aspectos clave de la propia vida se relaciona directamente con la privacidad. La teoría sugiere que el respeto a la privacidad es fundamental para preservar la autonomía de los individuos, permitiéndoles definir y seguir sus propios valores y objetivos. En un contexto democrático, la privacidad se considera un componente vital para el funcionamiento saludable del sistema.

Proteger la privacidad de los ciudadanos es esencial para evitar la manipulación y garantizar la diversidad de opiniones, lo que contribuye a un proceso democrático más robusto. Por ello sostiene que al proteger la privacidad, se promueve el desarrollo individual y social. El derecho a controlar la propia información personal permite a las personas experimentar, aprender y evolucionar sin una exposición constante y sin restricciones indebidas.

La privacidad se asocia con la capacidad de tomar riesgos, experimentar y ser creativo. En un entorno donde la privacidad está protegida, las personas pueden sentirse más libres para contribuir con nuevas ideas sin temor a la censura o al escrutinio excesivo. Este hecho conlleva a construir y mantener relaciones de confianza. La capacidad de compartir información de manera selectiva y controlada es fundamental para establecer relaciones significativas y duraderas. Esta teoría argumenta que, al salvaguardar la privacidad, se fomenta un entorno donde las personas pueden participar plenamente en la sociedad, ejercer sus derechos fundamentales, contribuir a la innovación y la creatividad, y participar de manera efectiva en procesos democráticos. En este sentido, la protección de datos personales no se ve solo como una medida de seguridad, sino como un medio para enriquecer y fortalecer los valores fundamentales de una sociedad.

La Teoría de la “Autenticidad e Integridad Personal” en el contexto de la protección de datos destaca la importancia de garantizar que la información recopilada y utilizada sobre un individuo no distorsione ni dañe su identidad real ni su integridad. La autenticidad se refiere a la verdad y fidelidad de la identidad de una persona. Esta teoría argumenta que la información personal recopilada

debe reflejar con precisión quién es la persona en la realidad. Cualquier manipulación o mal uso de estos datos que distorsione la verdadera identidad violaría esta autenticidad.

La teoría busca proteger a los individuos contra el uso indebido de sus datos personales que podría distorsionar su imagen pública o privada. Esto podría incluir la manipulación de datos para crear perfiles falsos, la difusión de información incorrecta o la utilización de datos de una manera que tergiverse la percepción pública de la persona. Para preservar la autenticidad e integridad personal, se argumenta que las personas deben dar su consentimiento informado para la recopilación y uso de sus datos. Esto implica que deben estar plenamente conscientes de cómo se utilizarán sus datos y dar su aprobación consciente. También desde esta perspectiva, se destaca la necesidad de que las entidades que recopilan datos sigan prácticas éticas en su tratamiento. Esto incluye el manejo responsable de datos, evitando prácticas invasivas o manipulativas que podrían afectar negativamente la percepción y autenticidad de un individuo.

La teoría respalda la idea de que los individuos deben tener el derecho de corregir cualquier información incorrecta sobre ellos y, en algunos casos, el derecho a que se eliminen ciertos datos que podrían afectar su integridad. La teoría también sugiere que las leyes y regulaciones deben ser diseñadas para prevenir el uso malicioso de datos que pueda dañar la autenticidad e integridad personal. Esto podría incluir medidas para prevenir el robo de identidad, la difamación en línea y otras formas de manipulación.

Cabe indicar que todas las teorías expuestas hacen hincapié en que el tratamiento de datos personales debe realizarse conforme a los requisitos y disposiciones establecidas en la ley. Es por ello que se consideran ciertos principios rectores como los son: la legalidad en su recopilación, el consentimiento en su tratamiento, la finalidad de su uso, la proporcionalidad en su tratativa, la calidad en su recopilación, la disposición de recurso de protección, el nivel de protección adecuado en su tratamiento y la seguridad en su administración y tratamiento (Anstis & Barnett, 2022a).

El principio de "Legalidad en la protección de datos personales" es fundamental en la regulación de la privacidad y el tratamiento de información personal. por eso se debe tener en cuenta la base legal específica el mismo que tiene su sustento en que cualquier procesamiento o tratamiento de datos personales debe tener una base legal clara y específica que lo respalde (González, 2020a). Esta base legal puede variar según la legislación aplicable, pero algunas de las bases legales comunes incluyen el consentimiento del titular, la ejecución de un contrato, el cumplimiento de una obligación legal, el interés legítimo del responsable del tratamiento, por mencionar algunos de ellos (Bonet Navarro, 2021a).

Es por ello que se debe contar con el consentimiento del titular; el mismo que es una de las bases legales más conocidas y utilizadas para el tratamiento de datos personales. Implica que el titular de los datos debe dar su autorización explícita, informada y libre para que sus datos sean procesados para una finalidad específica (Polo-Roca, 2020a). El consentimiento debe ser obtenido de

manera transparente, y el titular debe ser capaz de retirarlo en cualquier momento (Carrillo, 2021a).

En algunos casos, el tratamiento de datos personales puede ser necesario para cumplir con un contrato en el que el titular es parte o para cumplir con una obligación legal impuesta al responsable del tratamiento, tal es el caso de las obligaciones financieras o aduaneras (Serna, 2021c). Es por ello que debe existir el interés legítimo para su tratamiento. Este concepto se refiere a situaciones en las que el responsable del tratamiento puede tener un interés legítimo en procesar los datos, siempre que este interés no sea anulado por los derechos y libertades fundamentales del titular (Serna, 2021d). A esto se suma que el principio de legalidad también implica que el tratamiento de datos debe cumplir con las leyes y regulaciones aplicables en el país en el que se realiza, esto en el marco de la aplicación de la legislación vigente. En Perú, esto incluye la Ley de Protección de Datos Personales (Ley N° 29733) y su reglamento, que establecen las reglas y requisitos específicos para el tratamiento de datos personales en el país.

El responsable del tratamiento de datos personales tiene la responsabilidad de asegurarse de que cualquier procesamiento de datos se realice de manera legal y conforme a la base legal correspondiente (Blanco, 2022). Esto implica llevar a cabo evaluaciones de impacto en la protección de datos, obtener el consentimiento cuando sea necesario, implementar medidas de seguridad adecuadas y garantizar la transparencia en el uso de datos (Ziccardi, 2014).

Respecto al principio del “consentimiento en la tratativa de los datos personales” garantiza que el tratamiento de estos datos sea ético y respetuoso con los derechos de los individuos. Por ello se debe contar con la “autorización Informada” lo que significa que el titular de los datos debe recibir información clara y completa antes de dar su consentimiento (Jiménez & García-Ferrería, 2015). Esta información debe incluir detalles sobre quién está recopilando los datos, la finalidad del tratamiento, las categorías de datos que se recopilarán y cualquier otra información relevante. La persona debe comprender plenamente las implicaciones de dar su consentimiento. Se debe tener presente que cuando se trata de datos de menores de edad, el consentimiento debe obtenerse de sus padres o tutores legales, dependiendo de la legislación específica aplicable. Los menores generalmente no tienen la capacidad legal para dar un consentimiento válido por sí mismos (Díaz, 2023).

Asimismo el consentimiento debe ser libre y voluntario. No debe haber coerción, presión indebida o consecuencias negativas para el titular de los datos si decide no dar su consentimiento. Las personas deben tener la opción de negarse a dar su consentimiento sin sufrir represalias. Debemos remarcar por ello que el consentimiento debe ser específico para cada finalidad de tratamiento de datos. Esto significa que una organización no puede obtener un consentimiento general y luego usar los datos para cualquier propósito que desee. Debe obtenerse un consentimiento separado y específico para cada uso previsto de los datos personales (Awaghade, 2022).

Por otro lado, la posibilidad de revocación del consentimiento debe ser informada al titular de los datos con la finalidad de ejercer la capacidad de retirar

su consentimiento en cualquier momento (Susi, 2021). Esto significa que una vez que se haya otorgado el consentimiento, el titular puede decidir en cualquier momento que ya no desea que sus datos se utilicen para la finalidad específica y, en ese caso, la organización debe dejar de tratar esos datos para ese propósito (Morales & Lidette, 2022).

Es obligación de las organizaciones llevar un registro de los consentimientos obtenidos, incluyendo la fecha, la finalidad para la cual se otorgó el consentimiento y cómo se obtuvo. Este registro puede ser solicitado por las autoridades de protección de datos como evidencia de cumplimiento. Para efectos del registro se debe tomar en consideración que la información proporcionada al titular de los datos debe estar en un lenguaje claro y comprensible. Se debe evitar el uso de términos técnicos o jerga que pueda dificultar la comprensión de las implicaciones del consentimiento y así tener un consentimiento indubitable sobre el uso de los datos proporcionados (Siagian et al., 2023).

En el contexto digital, como en sitios web y aplicaciones móviles, es importante que las organizaciones utilicen métodos claros y transparentes para obtener el consentimiento en línea, como casillas de verificación (checkboxes) o botones de aceptación (Lugo & Ithurburu, 2020). Además, deben proporcionar enlaces a políticas de privacidad detalladas para que los usuarios puedan obtener más información si lo desean. El cumplimiento de estos aspectos en relación al principio del consentimiento es esencial para asegurarse de que el tratamiento de datos personales sea ético, legal y respetuoso con los derechos de privacidad de los individuos. Las organizaciones que no cumplen con estos

requisitos pueden enfrentar sanciones y multas significativas en virtud de las leyes de protección de datos (Vázquez-Cano & Pascual -Moscoso, 2022).

Con relación al principio de “finalidad en la protección de datos personales” es fundamental garantizar que el tratamiento de la información sea adecuado, transparente y respetuoso con la privacidad de los individuos. Por ello la recopilación para fines específicos y legítimos es primordial en su desarrollo. El responsable del tratamiento debe tener una razón válida y legal para recopilar estos datos. Por ejemplo, si una empresa recopila datos de sus clientes para procesar pedidos y entregar productos, esta es una finalidad específica y legítima (Jiménez & García-Ferrería, 2015).

Bolívar-Oñoro (2020), señaló que el responsable del tratamiento debe informar de manera transparente a los titulares de los datos sobre el propósito de la recopilación y el tratamiento de los datos. Esto implica que los individuos deben comprender por qué se están recopilando sus datos y cómo se utilizarán. Además, deben dar su consentimiento de manera informada y voluntaria para que los datos se utilicen de acuerdo con esa finalidad (Rallo, 2020). Asimismo, los datos personales no deben utilizarse de manera incompatible con la finalidad original para la que se recopilaron. Esto significa que si se recopilan datos para una finalidad específica, no se pueden utilizar para otro propósito sin el consentimiento adicional del titular de los datos. Por ejemplo, si una empresa recopila datos para enviar boletines informativos, no puede utilizar esos datos para publicidad sin el consentimiento previo del titular.

El principio de finalidad está relacionado con la minimización de datos. Esto implica que solo se deben recopilar los datos que sean estrictamente

necesarios para cumplir con la finalidad establecida. No se deben recopilar datos adicionales o innecesarios que no estén directamente relacionados con esa finalidad (Ganesan, 2022). Para asegurarse de que se cumple con este principio, las organizaciones y entidades que manejan datos personales deben conocer y cumplir con las leyes y regulaciones aplicables en materia de protección de datos. Esto incluye la Ley de Protección de Datos Personales de Perú y otras leyes nacionales e internacionales relacionadas con la privacidad y la protección de datos. El responsable del tratamiento de datos personales tiene la responsabilidad de garantizar que se respete este principio. Esto incluye la implementación de políticas y procedimientos adecuados, así como la capacitación del personal en cuestiones de protección de datos.

El principio de finalidad en la protección de datos personales busca garantizar que los datos se utilicen de manera justa, transparente y conforme a los deseos y expectativas de los titulares de los datos. Esto es esencial para proteger la privacidad y la seguridad de la información personal y para establecer una base de confianza entre las organizaciones y los individuos cuyos datos se manejan (Bonet-Navarro, 2021).

Respecto al principio de “origen y proporcionalidad en la tratativa de los datos personales”, se refiere a que el tratamiento de estos datos debe ser proporcionado y adecuado en relación con la finalidad para la cual fueron recopilados. El tratamiento de datos debe ser adecuado para alcanzar la finalidad específica para la cual se recopilaron los datos (Gázquez, 2022). Esto significa que el responsable del tratamiento debe evaluar cuidadosamente qué datos son necesarios y relevantes para cumplir con ese propósito particular. No se deben

recopilar más datos de los necesarios para lograr el objetivo deseado. Por otro lado, el tratamiento de datos personales debe ser necesario para cumplir con la finalidad establecida. Esto implica que, antes de recopilar cualquier dato, se debe considerar si existe una forma menos intrusiva o invasiva de lograr el mismo propósito. Si es posible alcanzar la finalidad sin recopilar datos personales, entonces no se deben recopilar (Rights, 2022).

Uno de los aspectos clave de este principio es la idea de evitar cualquier tipo de exceso en la recopilación y el tratamiento de datos personales. Esto significa que no se deben recopilar datos innecesarios o excesivos que no estén directamente relacionados con la finalidad establecida (Benoit, 2022). Asimismo, una forma práctica de aplicar el principio de proporcionalidad es practicar la minimización de datos. Esto implica recopilar solo la cantidad mínima de datos personales que sea necesaria para cumplir con la finalidad específica. Al hacerlo, se reduce el riesgo de recopilar información sensible o excesiva que pueda ser vulnerable a violaciones de seguridad o mal uso.

La evaluación constante de la proporcionalidad es esencial. A medida que evoluciona la finalidad del tratamiento de datos o cambian las circunstancias, es importante revisar y ajustar la recopilación y el tratamiento de datos para garantizar que sigan siendo proporcionados y necesarios. La evaluación constante por ende debe asegurar de que el tratamiento de datos personales sea equilibrado y no invasivo (Patraca et al., 2021). Esto protege la privacidad de los individuos al garantizar que solo se recopilen y se utilicen los datos necesarios para lograr una finalidad específica, evitando así cualquier exceso o recopilación innecesaria que pueda poner en riesgo la privacidad y la seguridad de los datos

personales. Este principio es un componente esencial de cualquier marco legal de protección de datos y que está incluida la legislación peruana.

Respecto al principio de “calidad en la protección de datos personales” esta es esencial para garantizar que la información recopilada y tratada sea precisa y confiable. Por ello los datos personales deben ser veraces, lo que significa que la información debe reflejar la realidad de la persona a la que se refiere. Esto implica que el responsable del tratamiento debe asegurarse de que los datos que recopila sean proporcionados de buena fe y que no contengan información falsa o engañosa (Ramírez & Vázquez, 2023). Además de ser veraces, los datos personales también deben ser exactos. Esto significa que la información debe ser precisa y no contener errores significativos. Es responsabilidad del responsable del tratamiento asegurarse de que los datos recopilados sean correctos y estén actualizados.

Los datos personales deben mantenerse actualizados. Esto implica que, si los datos cambian o dejan de ser precisos por algún motivo, el responsable del tratamiento debe tomar medidas para corregirlos o actualizarlos de manera oportuna. Los titulares de los datos también tienen la responsabilidad de notificar cualquier cambio en su información personal (Olivares, 2019).

Para cumplir con el principio de calidad, las organizaciones y entidades que tratan datos personales deben implementar las siguientes prácticas orientadas a que la forma como se gestionan los datos personales garanticen integridad y para ello se deben establecer ciertos lineamientos como lo son: la implementación de procedimientos de verificación, mantenimiento de registros actualizados, procedimientos de corrección, estrategias de educación y

capacitación del personal e implementación de políticas de retención de datos (Pineda et al., 2022).

Por otro lado, los procedimientos de verificación están orientados a que antes de recopilar datos, es importante verificar la autenticidad de la información proporcionada por los titulares. Esto puede incluir la verificación de documentos de identificación o la confirmación de datos con fuentes confiables (Pilege et al., 2022).

Los procedimientos de mantenimiento de registros actualizados orientan a que las organizaciones deben llevar un registro actualizado de los datos personales que poseen y asegurarse de que esta información se mantenga precisa a lo largo del tiempo (Polo-Roca, 2020b).

Los procedimientos de corrección deben establecerse con la finalidad de corregir datos inexactos o desactualizados cuando se detecten. Los titulares de los datos también deben tener la posibilidad de solicitar la corrección de sus datos si encuentran errores (Akrivopoulou, 2012).

Las estrategias de educación y capacitación del personal buscan que el personal que maneja datos personales debe estar capacitado y conscientes de la importancia de mantener la calidad de los datos. Esto incluye la formación en la identificación y corrección de posibles errores (González-Patiño & Esteban-Guitart, 2021).

La implementación de políticas de retención de datos busca que las organizaciones deben tener normas claras sobre cuánto tiempo conservarán los

datos personales y cómo manejan los datos obsoletos o innecesarios (Díaz, 2023).

El incumplimiento del principio de calidad puede tener consecuencias negativas tanto para los titulares de los datos como para las organizaciones que los tratan. Puede llevar a la toma de decisiones erróneas basadas en información incorrecta, lo que puede tener implicaciones legales y financieras. Por lo tanto, garantizar la calidad de los datos es un aspecto crítico de la gestión de datos personales en cumplimiento con las leyes de protección de datos (González, 2020b).

El principio de "Disposición de recurso" garantiza que los titulares de los datos tengan la capacidad de ejercer sus derechos y tomar medidas cuando sus datos personales sean tratados de manera irregular o cuando se violen sus derechos de privacidad. Bajo este principio establece que debe haber un mecanismo claro y accesible para que los titulares de datos ejerzan sus derechos en relación con sus datos personales (Lombarte, 2020b). Estos derechos pueden incluir el acceso a sus datos, la rectificación de información inexacta, la eliminación de datos innecesarios o la oposición al procesamiento en ciertas circunstancias.

Por ello se deben establecer mecanismos mediante los cuales los titulares de datos deben tener la capacidad de presentar quejas o reclamaciones cuando consideren que sus derechos de privacidad han sido violados o que el tratamiento de sus datos se ha realizado de manera irregular (Wu, 2005). Esto puede incluir situaciones en las que sus datos se hayan utilizado sin su consentimiento, se hayan compartido con terceros de manera inapropiada o se

hayan perdido debido a una falta de medidas de seguridad adecuadas (Milan & Velden, 2016).

En el contexto peruano, esto se traduce en la posibilidad de presentar acciones por la vía administrativa ante la Autoridad Nacional de Protección de Datos Personales (ANPDP). La ANPDP es la entidad encargada de supervisar y hacer cumplir las leyes de protección de datos en el país (Luna Cervantes, 2021a). Los titulares de datos pueden presentar quejas directamente ante esta autoridad, que tiene la capacidad de investigar y tomar medidas para resolver los problemas de privacidad. Además de las vías administrativas, los titulares de datos también pueden recurrir a la vía jurisdiccional, es decir, a los tribunales, para hacer valer sus derechos de protección de datos. Pueden presentar demandas civiles en los tribunales si consideran que sus derechos de privacidad han sido violados y desean buscar una compensación o una resolución legal. En caso de que se presente una queja o reclamación, ya sea ante la autoridad de protección de datos o ante los tribunales, se sigue un proceso de resolución de disputas. Esto implica una investigación para determinar si ha habido una infracción de las leyes de protección de datos y, en caso afirmativo, la imposición de sanciones o la reparación de los daños causados (Garcia & Perea, 2020).

El principio de disposición de recurso garantiza que los titulares de datos tengan medios efectivos para proteger sus derechos de privacidad y tomar medidas legales cuando sus datos personales sean tratados de manera inadecuada o se violen sus derechos. Esto refuerza la confianza en la protección de datos y promueve el cumplimiento de las leyes de privacidad por parte de las organizaciones que manejan datos personales (León et al., 2021).

El principio de "Nivel de protección adecuado transfronterizos" en el contexto de la protección de datos personales se refiere a la necesidad de garantizar que, al transferir datos personales más allá de las fronteras de un país, se mantenga un nivel mínimo de seguridad y privacidad de acuerdo con las leyes de protección de datos del país de origen del titular de los datos (Muñoz, 2021).

En el entorno de la globalización, es común que las organizaciones y empresas transmitan datos personales a través de las fronteras. Esto puede incluir datos personales de clientes, empleados u otras partes interesadas. Cuando los datos cruzan las fronteras, es importante asegurarse de que el nivel de protección de esos datos no se degrade significativamente. Los países tienen diferentes leyes y regulaciones en cuanto a la protección de datos personales (Rúa & Tapiero, 2021). Algunos países pueden tener leyes sólidas de protección de datos que garantizan la privacidad y la seguridad de los datos, mientras que otros pueden tener marcos legales menos estrictos o incluso carecer de ellos por completo (García & Perea, 2020).

Es por ello que cuando los datos personales se transfieren a un país con un nivel de protección de datos inferior al del país de origen, es necesario tomar medidas para garantizar que la protección de esos datos no se vea comprometida. Esto puede incluir la implementación de cláusulas contractuales específicas en los acuerdos de transferencia de datos o el uso de mecanismos de autorización como las Decisiones de Adecuación de la Comisión Europea o los Escudos de Privacidad (Privacy Shield) en el caso de las transferencias desde la Unión Europea (Ramiro, 2021). Es por ello que antes de realizar una transferencia internacional de datos, las organizaciones deben llevar a cabo una

evaluación de riesgos para determinar si el país de destino ofrece un nivel adecuado de protección de datos. Esto implica considerar factores como las leyes locales, la infraestructura de seguridad cibernética y la capacidad de las autoridades locales para hacer cumplir las leyes de protección de datos (Moreno Bobadilla, 2020a).

En algunos casos en específico, el titular de los datos puede otorgar su consentimiento informado para la transferencia de sus datos a un país con un nivel de protección de datos diferente. Sin embargo, este consentimiento debe ser explícito y basarse en una comprensión completa de los riesgos involucrados (Roca, 2020b). Es el responsable del tratamiento de la organización o entidad que realiza la transferencia internacional de datos el que debe garantizar que se mantenga un nivel adecuado de protección de datos. Esto incluye tomar medidas para proteger los datos durante la transferencia y estar preparado para abordar cualquier problema que surja en el país de destino (Carrillo, 2021b).

El principio de “seguridad en la protección de datos personales” es de vital importancia para garantizar la integridad, confidencialidad y disponibilidad de la información personal (Digital, 2019). El principio de seguridad establece que tanto el titular del banco de datos personales que es la entidad u organización que recopila y almacena los datos, que se configura como el encargado del tratamiento y la entidad que procesa los datos en nombre del titular; comparten la responsabilidad de garantizar la seguridad de los datos personales. Ambas partes deben tomar medidas adecuadas para proteger la información (Font, 2019).

Esto implica la implementación de medidas técnicas, como el uso de sistemas de cifrado para proteger los datos en tránsito y en reposo, la implementación de firewalls y sistemas de detección de intrusiones para prevenir el acceso no autorizado, y el establecimiento de controles de acceso para limitar quién puede acceder a los datos. Además de las medidas técnicas, se deben establecer medidas organizativas sólidas. Esto incluye la formación y concienciación del personal sobre la importancia de la seguridad de los datos, la designación de un oficial de protección de datos (DPO) para supervisar el cumplimiento de las normativas de protección de datos y la elaboración de políticas y procedimientos de seguridad de datos (Castellanos Claramunt, 2020b).

Una parte fundamental de la seguridad de datos es prevenir el acceso no autorizado. Esto implica proteger adecuadamente los sistemas y redes que almacenan y procesan datos personales para evitar intrusiones y ataques cibernéticos. Asimismo se deben establecer procedimientos de copia de seguridad y recuperación de datos en caso de pérdida o daño de la información. Esto garantiza que los datos puedan ser restaurados en caso de eventos catastróficos, como fallos de hardware o ataques de ransomware (Digital, 2019).

Como lo señala Minero (2014), la implementación de registros de auditoría y control de acceso ayuda a realizar un seguimiento de las actividades relacionadas con los datos personales. Esto permite detectar y responder a actividades sospechosas o no autorizadas. Por ello es importante realizar evaluaciones regulares de riesgos para identificar posibles amenazas y vulnerabilidades en el tratamiento de datos personales. Esto permite tomar

medidas preventivas para mitigar los riesgos identificados. En caso de una violación de la seguridad que pueda poner en peligro la privacidad de los datos personales, se deben notificar estas brechas a las autoridades de supervisión y, en algunos casos, a los titulares de los datos, de acuerdo con las regulaciones de notificación de brechas de seguridad de datos aplicables (Heras, 2020).

El incumplimiento de las medidas de seguridad puede resultar en sanciones significativas y daños a la reputación de una organización, por lo que es esencial que tanto los titulares de datos como los encargados del tratamiento estén completamente comprometidos con la implementación y el mantenimiento de prácticas de seguridad robustas (González, 2017). La seguridad de los datos personales es un aspecto crucial de la protección de la privacidad y debe ser una prioridad en cualquier entidad que maneje este tipo de información.

II.4. Definición de Términos

- **Datos personales:**

Los "datos personales" se refieren a información que puede vincularse directa o indirectamente con una persona en particular. Esto incluye detalles como nombres, direcciones, números de identificación, información de contacto y datos biométricos, como huellas dactilares o rasgos faciales. Estos datos son esenciales para la identificación y comunicación de individuos, pero también deben ser manejados con cuidado y protegidos para garantizar la privacidad y la seguridad de las personas en un mundo digital en constante evolución. La gestión adecuada de los datos personales es un aspecto fundamental de la protección de la privacidad y los derechos digitales (Berrocal-Lanzarot, 2020).

- **Consentimiento informado:**

El "consentimiento informado" es un principio fundamental en la protección de datos personales. Este concepto se refiere al permiso otorgado por una persona para que sus datos personales sean procesados, pero con una condición esencial: este permiso solo es válido cuando la persona ha sido completamente informada sobre cómo se utilizarán sus datos. Toda persona debe estar plenamente consciente de cómo se recopilarán, almacenarán y utilizarán sus datos personales antes de otorgar su consentimiento. Esto implica que la información proporcionada debe ser clara, comprensible y detallada, de modo que la persona pueda tomar una decisión informada sobre si desea que sus datos sean procesados. El consentimiento informado es crucial para garantizar la privacidad y la autodeterminación de las personas en el entorno digital. Les brinda el control sobre su información personal y la capacidad de tomar decisiones informadas sobre su privacidad en línea. Además, en muchos sistemas legales, la falta de consentimiento informado puede llevar a consecuencias legales, como violaciones de la privacidad y sanciones para quienes recopilan datos sin permiso o de manera engañosa (Berrocal-Lanzarot, 2020)..

- **Privacidad:**

La privacidad es un derecho fundamental que garantiza que las personas tengan el control sobre su información personal y que puedan decidir quién tiene acceso a ella. Este derecho implica que los individuos tienen la capacidad de mantener ciertos aspectos de sus vidas, como datos personales, comunicaciones y actividades, lejos de la mirada pública o de terceros no autorizados. La

privacidad es esencial para proteger la autonomía, la dignidad y la libertad de las personas en un mundo cada vez más digital (Berrocal-Lanzarot, 2020)..

Este derecho les permite a las personas determinar qué información personal desean compartir y con quién. Pueden optar por mantener en privado detalles sobre su identidad, ubicación, preferencias, historial médico u otras cuestiones sensibles. La privacidad también se relaciona con la protección de datos personales, como números de identificación, direcciones y detalles de tarjetas de crédito, y asegura que estos datos estén resguardados de posibles abusos (Berrocal-Lanzarot, 2020).

En la era digital, la privacidad en línea se ha convertido en un tema crítico, ya que las actividades en la web dejan rastros de información personal. La privacidad en línea implica el control de los datos que compartimos en plataformas digitales y la prevención de la recopilación no autorizada de información. La legislación de protección de datos y las políticas de privacidad en línea desempeñan un papel fundamental en la preservación de este derecho en el entorno digital (Baz Rodríguez, 2019).

- **Brecha de datos:**

Una "brecha de datos" se refiere a un incidente en el que se produce un acceso no autorizado, divulgación o pérdida de datos personales debido a una vulneración de la seguridad. En otras palabras, cuando los datos personales, como información de identificación, detalles de tarjetas de crédito o información de salud, se exponen o se ponen en manos equivocadas debido a una falla en las medidas de seguridad, se considera una brecha de datos.

Estas brechas pueden ocurrir de diversas formas, como ataques cibernéticos, pérdida física de dispositivos de almacenamiento, errores humanos o incluso el robo de información. Las consecuencias de una brecha de datos pueden ser graves, ya que puede resultar en el robo de identidad, fraudes financieros o daño a la privacidad de las personas afectadas. Por lo tanto, la seguridad de datos y la prevención de brechas son cuestiones críticas en la era digital. Las organizaciones y empresas a menudo están legalmente obligadas a notificar a las personas afectadas cuando ocurre una brecha de datos y a tomar medidas para mitigar los efectos adversos (Etxebarria, 2019).

- **Cifrado:**

El cifrado es un proceso fundamental en la seguridad de la información en línea. Consiste en convertir datos en un formato ilegible a simple vista, conocido como texto cifrado, para proteger su confidencialidad. Solo las personas autorizadas, que poseen la clave de descifrado adecuada, pueden revertir este proceso y leer la información en su forma original (Berrocal-Lanzarot, 2020).

Este método es esencial para garantizar que los datos sensibles, como contraseñas, información financiera o mensajes privados, no sean accesibles para personas no autorizadas. El cifrado se utiliza en una amplia variedad de aplicaciones, desde la comunicación en línea y el comercio electrónico hasta el almacenamiento en la nube y la seguridad de dispositivos. Su objetivo es prevenir el acceso no autorizado y proteger la privacidad de los datos, incluso si alguien intenta interceptarlos durante la transmisión o acceder a ellos de manera no autorizada (Fernández, 2022; Samper, 2020).

- **Anonimización:**

La anonimización es un proceso fundamental en la protección de datos personales y la privacidad en línea. Consiste en eliminar o modificar cuidadosamente cualquier información que pueda identificar a una persona en un conjunto de datos, lo que garantiza que los datos se vuelvan anónimos. Esto significa que, una vez anonimizados, los datos ya no están vinculados a una persona en particular (Samper, 2020).

La anonimización es importante porque permite que los datos se utilicen con fines legítimos, como investigaciones estadísticas o análisis, sin exponer la identidad de las personas involucradas. Este proceso se realiza mediante la eliminación de elementos de identificación, como nombres, direcciones o números de identificación, o mediante la alteración de estos datos de tal manera que no se puedan relacionar con personas específicas.

Sin embargo, es esencial entender que la anonimización no garantiza la total privacidad, ya que en algunos casos, con técnicas avanzadas, aún es posible identificar a individuos a partir de datos anonimizados si se cruzan con otros datos disponibles públicamente. Por lo tanto, se debe aplicar con precaución y de acuerdo con las regulaciones de protección de datos para garantizar la privacidad y la seguridad de las personas (Fernández, 2022).

- **Derecho al olvido:**

El "Derecho al olvido" es un concepto fundamental en la protección de datos y la privacidad en línea. Este derecho le otorga a una persona el poder de solicitar la eliminación de sus datos personales que se encuentran en línea en ciertas

situaciones. Esto significa que, si una persona considera que la información sobre ella en internet es obsoleta, inexacta, irrelevante o perjudicial, puede pedir que se elimine o se limite su acceso (Font, 2019).

Este derecho se basa en el principio de que las personas deben tener control sobre su información personal y no deben estar perpetuamente expuestas a datos que puedan dañar su reputación o privacidad. Sin embargo, este derecho no es absoluto y está sujeto a ciertas limitaciones, como el interés público o la libertad de expresión. En general, el "Derecho al olvido" busca equilibrar la protección de la privacidad individual con otros derechos y valores en la sociedad digital

- **Ciberseguridad:**

La ciberseguridad se refiere a un conjunto de prácticas y tecnologías diseñadas para proteger sistemas, redes y datos en línea contra amenazas y ataques cibernéticos. Su objetivo principal es garantizar la confidencialidad, la integridad y la disponibilidad de la información digital (Fernández, 2022).

Para lograr esto, la ciberseguridad implica medidas como el uso de cortafuegos y sistemas de detección de intrusiones para prevenir y detectar intrusiones no autorizadas en redes. También involucra el cifrado de datos para proteger la información sensible de accesos no autorizados.

Además, la ciberseguridad incluye prácticas como la gestión de contraseñas seguras y la educación de usuarios para que estén alerta a las amenazas en línea, como el phishing. En un mundo cada vez más digital, la ciberseguridad se ha vuelto esencial para proteger a las organizaciones y las

personas de ataques que podrían resultar en la pérdida de datos, el robo de información confidencial o el daño a la infraestructura digital.

- **Protección de datos del consumidor:**

La "Protección de datos del consumidor" se refiere a un conjunto de leyes y regulaciones diseñadas para otorgar a los consumidores un mayor control sobre sus datos personales y su privacidad en línea. Estas leyes establecen los derechos y las normas que las empresas y organizaciones deben seguir al recopilar, procesar y almacenar datos personales de los consumidores (Fernández, 2022).

La protección de datos del consumidor busca garantizar que las empresas y las organizaciones manejen los datos personales de manera transparente y segura, obteniendo el consentimiento informado de los consumidores y permitiéndoles acceder a sus datos, corregirlos o solicitar su eliminación. Estas regulaciones son fundamentales en un entorno digital en constante evolución para preservar la privacidad y la seguridad de los consumidores en línea.

- **Identidad digital:**

La "identidad digital" es la representación en línea de una persona en el mundo digital. Incluye una variedad de elementos, como perfiles en redes sociales, cuentas de correo electrónico, registros en sitios web y otros datos digitales que están asociados a esa persona. En esencia, es cómo una persona se presenta y se relaciona en el entorno en línea (Berrocal-Lanzarot, 2020).

Esta identidad digital puede ser tan diversa como la persona misma, ya que refleja su presencia en la web. Los perfiles de redes sociales, por ejemplo, contienen información personal, publicaciones, fotos y conexiones con otras personas. Las cuentas de correo electrónico almacenan comunicaciones personales y profesionales. Los registros en sitios web pueden incluir historiales de compras, comentarios y más.

La identidad digital se ha vuelto cada vez más importante en la era digital, ya que afecta la forma en que las personas interactúan, se comunican y son percibidas en línea. Al mismo tiempo, la protección de esta identidad digital y la gestión adecuada de los datos asociados se han convertido en cuestiones críticas para la privacidad y la seguridad en línea. Por lo tanto, comprender y proteger la identidad digital es esencial en el mundo digital actual.

- **DPO (Delegado de Protección de Datos):**

El DPO (Delegado de Protección de Datos) es un profesional cuya responsabilidad principal es asegurar que una organización cumpla con todas las regulaciones y normativas relacionadas con la protección de datos personales. Su función es vital en un entorno donde la privacidad y la seguridad de los datos son fundamentales (Fernández, 2022).

Este experto supervisa y coordina todas las actividades relacionadas con la protección de datos dentro de la organización. Esto implica asesorar a la empresa sobre las mejores prácticas de privacidad, supervisar la implementación de políticas de privacidad, garantizar que se obtenga el consentimiento adecuado para el procesamiento de datos y actuar como punto

de contacto entre la organización y las autoridades reguladoras de protección de datos.

El DPO también se encarga de informar a los empleados y la dirección sobre las obligaciones de cumplimiento, así como de realizar auditorías y evaluaciones de impacto en la protección de datos. Su objetivo principal es asegurarse de que los datos personales se manejen de manera ética, segura y legal, brindando a las personas un mayor control sobre su información personal.

- **Big Data:**

El término "Big Data" se refiere a la práctica de analizar conjuntos masivos de datos con el propósito de descubrir patrones, tendencias y conocimientos significativos. Estos conjuntos de datos suelen ser extremadamente grandes y complejos, lo que hace que su análisis con enfoques tradicionales sea difícil o imposible. El análisis de Big Data implica el uso de tecnologías avanzadas para procesar, almacenar y examinar estos datos en busca de información valiosa. Este enfoque se utiliza en una amplia variedad de campos, desde el análisis de mercado y la investigación científica hasta la toma de decisiones empresariales y la predicción de tendencias. El objetivo es aprovechar la gran cantidad de datos disponibles en la era digital para obtener información que de otro modo pasaría desapercibida (Rank & Berberi, 2022).

Las aplicaciones de Big Data son diversas y van desde el análisis de las interacciones de los usuarios en redes sociales hasta la monitorización de sensores en dispositivos IoT. A medida que se generan más datos en el mundo digital, el análisis de Big Data se ha convertido en una herramienta poderosa

para entender y tomar decisiones basadas en datos. Sin embargo, también plantea desafíos, como la privacidad y la seguridad de los datos, que deben abordarse cuidadosamente en su implementación(Rank & Berberi, 2022).

- **Internet de las Cosas (IoT):**

El Internet de las Cosas (IoT) es un concepto que se refiere a una red interconectada de dispositivos físicos que están diseñados para recopilar y compartir datos entre sí a través de internet. Estos dispositivos pueden abarcar una amplia gama de objetos cotidianos, como termostatos, electrodomésticos, vehículos, sensores de seguridad y más. La idea central del IoT es que estos dispositivos pueden comunicarse entre sí y con sistemas centrales a través de internet, lo que permite recopilar información en tiempo real, tomar decisiones automatizadas y ofrecer a los usuarios un mayor control y comodidad en sus vidas. Sin embargo, este nivel de interconexión plantea desafíos significativos en términos de seguridad y privacidad, ya que la recopilación y transmisión de datos en IoT pueden generar preocupaciones sobre quién accede a esta información y cómo se utiliza. Por lo tanto, la gestión adecuada de la seguridad y la privacidad es esencial en el contexto del IoT (Anstis & Barnett, 2022b).

- **Perfilado:**

El perfilado es un proceso en el que se utilizan datos para crear perfiles detallados de usuarios en línea. Esto implica recopilar información sobre las actividades, preferencias y comportamientos de una persona en el mundo digital. Una vez que se ha creado un perfil, se puede utilizar para personalizar la publicidad, el contenido y las recomendaciones en línea, lo que significa que los

usuarios reciben anuncios y contenidos que se adaptan a sus intereses y comportamientos previos. El perfilado se utiliza en redes sociales, motores de búsqueda, plataformas de transmisión de video y muchas otras aplicaciones en línea para mejorar la experiencia del usuario y aumentar la relevancia de los contenidos y anuncios que se le presentan (Kirchschlaeger, 2019).

Sin embargo, el perfilado también plantea cuestiones de privacidad, ya que la recopilación y el uso de datos personales pueden generar preocupaciones sobre la privacidad y la seguridad de la información. Por lo tanto, las regulaciones de protección de datos, como el RGPD en la Unión Europea, imponen restricciones y requisitos específicos sobre cómo se puede llevar a cabo el perfilado y cómo se deben proteger los derechos de privacidad de los individuos.

- **Privacidad por diseño:**

Es un enfoque fundamental en la gestión de datos y la creación de productos y servicios. Implica que desde el inicio de cualquier proyecto, ya sea un software, una aplicación, un sistema en línea o cualquier otro producto o servicio, se deben considerar la protección de datos y la privacidad como componentes esenciales (Ballarín et al., 2021).

En otras palabras, la privacidad por diseño exige que, desde el momento en que se concibe una idea o proyecto, se deben tomar medidas para garantizar que la información personal de los usuarios se maneje con el máximo cuidado y respeto. Esto incluye la incorporación de medidas de seguridad sólidas, la limitación de la recopilación de datos a lo estrictamente necesario para lograr los

objetivos del producto o servicio, y la consideración de la privacidad del usuario en el diseño y la funcionalidad.

Este enfoque proactivo no solo garantiza el cumplimiento de las leyes de protección de datos, sino que también contribuye a construir la confianza del usuario y a prevenir problemas de seguridad y violaciones de privacidad en el futuro. En resumen, la privacidad por diseño busca incorporar la protección de datos y la privacidad en el ADN de cualquier producto o servicio, desde su concepción hasta su implementación, para garantizar que se respeten los derechos de privacidad de los usuarios.

- **Autoridad de Protección de Datos:**

La "Autoridad de Protección de Datos" es un organismo gubernamental encargado de garantizar el cumplimiento de las leyes y regulaciones relacionadas con la protección de datos y la privacidad. Su función principal es supervisar y hacer cumplir las políticas y normativas que protegen la información personal de los individuos (Alvear Richards & Hernández Pesantes, 2023).

Esta autoridad tiene la responsabilidad de velar por que las organizaciones y entidades, tanto del sector público como privado, cumplan con las leyes de protección de datos. Esto incluye asegurarse de que se recopilen, almacenen, procesen y compartan datos personales de acuerdo con las regulaciones aplicables. También puede brindar orientación, emitir directrices y, en algunos casos, imponer sanciones a las organizaciones que no cumplan con las leyes de protección de datos.

La Autoridad de Protección de Datos desempeña un papel fundamental en la preservación de la privacidad y la seguridad de la información personal en la era digital. Su labor contribuye a mantener un equilibrio entre la recopilación y el uso de datos personales y la protección de los derechos individuales en un entorno cada vez más interconectado y digital.

- **Cookies:**

Las "cookies" son pequeños archivos de texto que los sitios web guardan en tu dispositivo cuando navegas por internet. Estos archivos contienen información sobre tu actividad en línea y se utilizan para diversas finalidades. Por ejemplo, las cookies pueden recordar tus preferencias en un sitio web, como el idioma o la ubicación, para hacer tu experiencia de navegación más personalizada (Serna, 2021b) .

Además, las cookies son utilizadas para rastrear tu actividad en línea. Esto puede incluir información sobre las páginas que visitas, cuánto tiempo permaneces en un sitio y tus patrones de navegación. Los datos recopilados a través de las cookies a menudo se utilizan para analizar el comportamiento del usuario y ofrecer publicidad dirigida.

Es importante destacar que existen diferentes tipos de cookies, algunas de las cuales son esenciales para el funcionamiento de un sitio web, mientras que otras se utilizan con fines analíticos o publicitarios. Sin embargo, las cookies también han generado preocupaciones sobre la privacidad, ya que pueden rastrear la actividad de los usuarios en línea. Por esta razón, las regulaciones de privacidad, como el Reglamento General de Protección de Datos (RGPD) de la

Unión Europea, requieren que los sitios web informen a los usuarios sobre el uso de cookies y obtengan su consentimiento antes de almacenar estas en sus dispositivos(Serna, 2021a).

- **Firma digital:**

La firma digital es un método de autenticación electrónica que se utiliza para verificar tanto la integridad como la autoría de un documento o mensaje en el entorno digital. Esto se logra a través de un proceso de codificación que crea una firma única y cifrada, que se adjunta al documento o mensaje. Cuando alguien firma digitalmente un documento o mensaje, el sistema utiliza una clave privada para generar una firma digital exclusiva para ese contenido específico (Ibarra, 2023). La firma se basa en el contenido del documento, lo que significa que si el documento se altera de alguna manera, la firma ya no coincidirá, lo que garantiza la integridad del contenido. Además, la firma digital se puede verificar utilizando la clave pública del remitente, lo que confirma la autoría del documento o mensaje. Esto proporciona un alto nivel de seguridad y confianza en la autenticidad del contenido y en la identidad del remitente.

- **Derechos digitales:**

Los "Derechos Digitales" se refieren a un conjunto de derechos que buscan proteger a las personas en el entorno digital o en línea. Estos derechos son fundamentales en la era digital y abordan cuestiones esenciales como la privacidad, la libertad de expresión y la seguridad en Internet. La privacidad dentro de los derechos digitales garantiza que las personas tengan el control sobre su información personal en línea. Esto implica que los datos personales

no deben ser recopilados, utilizados o compartidos sin el consentimiento informado del individuo(Castellanos Claramunt, 2020b). La privacidad también se relaciona con la capacidad de mantener la confidencialidad de la comunicación y la actividad en línea. Por otro lado la libertad de expresión es importante en un mundo digital, la libertad de expresión permite a las personas expresar sus opiniones, ideas y creencias en línea sin censura indebida. Esto es fundamental para la democracia y la diversidad de pensamiento en la sociedad. También se debe tomar en consideración la seguridad en línea, esto debido a que los derechos digitales incluyen la protección contra amenazas cibernéticas y delitos en línea. Esto implica medidas para garantizar la seguridad de la información personal y la integridad de los sistemas en línea.

III. HIPOTESIS Y VARIABLES

III.1. Hipótesis

- **Hipótesis General**

H0: No existe relación entre la protección de datos personales y los derechos digitales en el Perú.

H1: Existe relación entre la protección de datos personales y los derechos digitales en el Perú

- **Hipótesis específicas**

Hipótesis específica 01

H0: No existe relación entre la protección de datos personales y la privacidad y confidencialidad digital en el Perú.

H1: Existe relación entre la protección de datos personales y la privacidad y confidencialidad digital en el Perú

Hipótesis específica 02

H0: No existe relación entre la protección de datos personales y el derecho al olvido digital en el Perú.

H1: Existe relación entre la protección de datos personales y el derecho al olvido digital en el Perú.

Hipótesis específica 03

H0: No existe relación entre la protección de datos personales y derecho a la identidad digital en el Perú.

H1: Existe relación entre la protección de datos personales y derecho a la identidad digital en el Perú.

Hipótesis específica 04

H0: No existe relación entre la protección de datos personales y derecho a la educación digital en el Perú.

H1: Existe relación entre la protección de datos personales y derecho a la educación digital en el Perú.

III.2. Variables

Respecto a la primera variable de “Protección de datos personales”, se refiere al conjunto de medidas y regulaciones establecidas para salvaguardar la privacidad y la información personal de individuos en entornos digitales y no digitales. Esta variable abarca la recopilación, el almacenamiento, el procesamiento y la transmisión de datos que están relacionados con personas, ya sean datos identificables, como nombres y números de identificación ante entidades públicas o gubernamentales, o datos sensibles, como información médica o financiera.

La protección de datos personales se basa en la premisa de que las personas tienen el derecho fundamental a mantener el control sobre su

información personal y decidir cómo se utiliza. Por lo tanto, esta variable implica la implementación de salvaguardias técnicas, legales y organizativas para prevenir la divulgación no autorizada, el robo de datos, el abuso de la información personal y garantizar que se utilicen solo para fines legítimos y consensuados.

En un entorno digital, la protección de datos personales se ha vuelto especialmente relevante debido a la creciente cantidad de información personal que se genera y comparte en línea. Los marcos legales y las regulaciones buscan garantizar la protección de datos personales en un mundo cada vez más digitalizado. La violación de esta variable puede dar lugar a sanciones legales y daños a la privacidad de las personas, lo que subraya su importancia en la sociedad moderna.

Respecto a la segunda variable “Derechos digitales” se refiere a un conjunto de derechos fundamentales que protegen a las personas en el entorno digital o cibernético. Estos derechos son una extensión de los derechos humanos tradicionales hacia el mundo en línea y se centran en salvaguardar la privacidad, la libertad de expresión, la seguridad y otros aspectos clave de la vida digital.

En la era digital, los derechos digitales son esenciales para garantizar que las personas tengan la capacidad de ejercer sus libertades y proteger su información personal en línea. Esto incluye el derecho a la privacidad de datos, que otorga a las personas el control sobre cómo se recopilan y utilizan sus datos personales en internet. También incluye el derecho a la libertad de expresión en línea, que permite a las personas expresar sus opiniones y acceder a información en la red sin censura indebida.

Los derechos digitales también abordan cuestiones de seguridad en línea, asegurando que las personas estén protegidas contra delitos cibernéticos y amenazas a su identidad digital. Estos derechos son cruciales en una sociedad cada vez más conectada digitalmente, ya que garantizan que las personas puedan participar plenamente en el mundo en línea sin temor a violaciones de su privacidad o a la censura de sus opiniones.

III.3. Operacionalización de las variables

Variable 1: Protección de datos personales

Respecto a la variable Protección de datos personales se refiere a las medidas y prácticas destinadas a resguardar la información que identifica o puede identificar a una persona. Estas medidas buscan asegurar que los datos personales, como nombres, direcciones, números de teléfono y cualquier otra información privada, se manejen de manera segura y se utilicen de acuerdo con las leyes y regulaciones pertinentes. El objetivo es salvaguardar la privacidad y la seguridad de los individuos, controlando el acceso, uso, divulgación y tratamiento de sus datos personales por parte de organizaciones y entidades.

Para su desarrollo se han tomado en consideración las siguientes dimensiones:

- Dimensión 1: Seguridad y protección
- Dimensión 2: Finalidad legítima y limitada
- Dimensión 3: Consentimiento informado

En la primera dimensión, centrada en la seguridad y protección de datos, se evalúan diversos indicadores clave. Se considera la existencia de medidas tecnológicas como el cifrado de datos, cortafuegos y antivirus para salvaguardar la información personal. Además, se valora la capacitación regular del personal en prácticas de seguridad de datos y la conciencia de las amenazas cibernéticas. El registro y seguimiento de incidentes de seguridad, la evaluación periódica de vulnerabilidades, y las auditorías de seguridad se destacan como elementos esenciales. El cumplimiento de estándares reconocidos, como ISO 27001 o normativas sectoriales específicas, también se toma en cuenta.

En la segunda dimensión, relacionada con la finalidad legítima y limitada del procesamiento de datos, se examinan indicadores que abordan la claridad en la documentación de los propósitos de recopilación de datos personales. Se valora la revisión periódica de la idoneidad de estos propósitos, así como la implementación de políticas que prohíban el uso no autorizado de datos personales. Los procedimientos de revisión en caso de cambios en las circunstancias y la verificación del tiempo de almacenamiento de datos según los fines declarados son elementos clave de evaluación.

La tercera dimensión, enfocada en el consentimiento informado, analiza la obtención de consentimiento claro y específico de los titulares de datos antes de recopilar o procesar sus datos personales. La documentación detallada de los procedimientos utilizados para obtener y registrar el consentimiento es fundamental. Asimismo, se evalúa la garantía de que los titulares estén debidamente informados sobre el uso previsto de sus datos personales. La provisión de mecanismos para retirar el consentimiento en cualquier momento y

la renovación del mismo ante cambios en los fines de procesamiento de datos son aspectos clave en esta dimensión.

Variable 2: Derechos digitales

Respecto a la variable Derechos digitales se refieren a los principios y garantías que salvaguardan las libertades y protecciones fundamentales de las personas en el entorno digital. Estos derechos abarcan cuestiones como la privacidad en línea, la libertad de expresión en plataformas digitales, el acceso equitativo a la información, la seguridad de los datos personales y la no discriminación en el ámbito digital. En esencia, los derechos digitales buscan establecer un marco normativo que proteja los valores democráticos y los derechos humanos en el contexto de la tecnología y la comunicación digital.

Para su desarrollo se han tomado en consideración las siguientes dimensiones:

- Dimensión 1: Privacidad y confidencialidad
- Dimensión 2: Derecho al olvido
- Dimensión 3: Derecho a la identidad digital
- Dimensión 4: Derecho a la educación digital

En la primera dimensión, centrada en Privacidad y Confidencialidad, se consideran elementos como la proporción de usuarios que ajustan configuraciones de privacidad en plataformas en línea, el número de denuncias de violaciones de privacidad, el grado de conciencia pública sobre prácticas de recolección y uso de datos, así como la implementación de regulaciones de protección de datos y sus efectos.

La segunda dimensión, relacionada con el Derecho al Olvido, se evalúa mediante indicadores como el número de solicitudes de eliminación de información personal en motores de búsqueda, la tasa de cumplimiento de estas solicitudes, la efectividad de la eliminación en la restauración de la privacidad y reputación en línea, así como la resolución de casos controversiales vinculados a este derecho.

La tercera dimensión, enfocada en el Derecho a la Identidad Digital, incluye aspectos como el nivel de autenticación y verificación requerido para acceder a servicios digitales, casos de robo de identidad digital, medidas de seguridad en la gestión de identidades digitales (como la autenticación de dos factores) y la tasa de adopción de sistemas de gestión de identidades digitales descentralizadas.

Por último, cuarta dimensión, que aborda el Derecho a la Educación Digital, considera variables como el acceso a la educación digital (incluyendo acceso a Internet y dispositivos para la educación en línea), la inversión en programas de alfabetización digital y educación en línea, la evaluación de la calidad y disponibilidad de contenido educativo en línea, y la participación y finalización de cursos y programas de educación digital.

La escala de evaluación, en este caso, es ordinal, con niveles que van desde "Totalmente en desacuerdo" hasta "Totalmente de acuerdo" en una escala Likert tomando valores del 1 al 5.

IV. MATERIALES Y METODOS

IV.1. Área de estudio

Respecto a la unidad de estudio se ha considerado a la ciudad de Lima. Esta selección obedece a la cantidad de organización público y privadas realizan actividades en el indicado entorno geográfico

IV.2. Diseño de Investigación

En la era digital actual, la creciente interconexión de las sociedades ha llevado a una explosión en la generación, recolección y procesamiento de datos personales. En este contexto, la protección de datos personales emerge como una preocupación central, especialmente cuando se examina su relación con la identidad digital. La identidad digital, entendida como la representación en línea de una persona, se ha vuelto integral para la participación en la sociedad contemporánea. Esta conexión entre la protección de datos y la identidad digital es un fenómeno complejo que requiere un análisis socio-jurídico detallado y exhaustivo.

Desde el ámbito jurídico, la protección de datos personales se ha convertido en un tema de importancia crítica. En muchos países, incluido Perú, se han implementado leyes y regulaciones para salvaguardar la privacidad de los individuos y controlar la recopilación y el uso de sus datos. Investigar cómo estas leyes se aplican específicamente a la identidad digital, que a menudo trasciende fronteras físicas, es esencial. Se requiere un análisis de la legislación vigente en Perú y su adecuación para abordar los desafíos particulares que plantea la identidad digital.

Desde una perspectiva social, la identidad digital no solo abarca la forma en que los individuos son percibidos en línea, sino también cómo la información personal puede influir en las oportunidades y experiencias de la vida cotidiana. Por lo tanto, investigar la relación entre la protección de datos y la identidad digital implica comprender cómo estas interacciones afectan la autonomía, la inclusión y la equidad en la sociedad peruana. ¿Existen desigualdades en la protección de datos y, por ende, en la construcción de identidades digitales?

Además, el avance tecnológico constante introduce desafíos adicionales. Las tecnologías emergentes, como la inteligencia artificial y el análisis de “bigdata”, plantean preguntas cruciales sobre cómo se manejarán los datos personales en el futuro. Una exploración socio-jurídica debe considerar estos desarrollos y proponer posibles marcos regulatorios y éticos.

Una investigación en esta área no solo contribuirá a la academia y al desarrollo de políticas, sino que también proporcionará información valiosa para los ciudadanos y las empresas en Perú. La comprensión de cómo se entrelazan la protección de datos y la identidad digital es esencial para garantizar un entorno digital justo, seguro y respetuoso en el país.

El tipo de Investigación, según su finalidad, fue del tipo básica, ello porque se buscó determinar una relación entre las variables de estudio propuestas, de modo que se continúe estudiando a mediano plazo, para mejorar la protección de los datos y su relación con los derechos digitales.

La investigación básica también conocida como investigación teórica, pura o fundamental. Ya que está destinada a aportar un cuerpo organizado de

conocimientos científicos y no produce necesariamente resultados de utilidad práctica inmediata. Se preocupa por recoger información de la realidad para enriquecer el conocimiento teórico-científico, orientado al descubrimiento de principios y leyes. (Valderrama, 2013, p. 64)

El diseño de investigación se realizó en base a un diseño no experimental: de corte transversal, de nivel correlacional. Ello porque la recolección de la información se realizó en un solo espacio y momento, con la finalidad de describir y analizar adecuadamente las variables presentadas para investigación.

Los diseños no experimentales son estudios que se realizan sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para analizarlos. (Hernandez, Fernandez y Baptista, 2014, p.152).

Los diseños transversales se dan cuando los datos son recopilados en un solo momento y son transversales descriptivos cuando indagan la incidencia de las modalidades, categorías o niveles de una o más variables en una población es decir ubica a un grupo de estudio (personas, fenómenos, situaciones, u otros) en una variable para describir el procedimiento (Hernandez, Fernandez y Baptista)

IV.3. Población y muestra

Población:

Esta investigación consideró como población a 20,000 ciudadanos que son usuarios de distintos servicios de la administración pública o privada en la que han brindado sus datos de manera voluntaria.

- Criterios de inclusión: Ciudadanos mayores de edad y que son usuarios de los servicios privados o gubernamentales los cuales tienen acceso y custodia a los datos personales por ellos otorgados.
- Criterios de exclusión: Ciudadanos que son funcionarios públicos a privados en los cuales se realicen actividades de procesamiento o custodia de los datos brindados por los encuestados.

Muestra:

Esta investigación, estuvo representada por 378 personas seleccionadas de manera aleatoria entre los ciudadanos que son usuarios de distintos servicios de la administración pública o privada. Para obtener el tamaño de la muestra se utilizó la ecuación estadística para proporciones poblacionales, considerando un nivel de confianza del 95%, nivel de error de 0.05 y una población de 20000 personas; los cálculos se realizaron de acuerdo a la siguiente formula:

$$n = \frac{z^2(p \cdot q)}{e^2 + \frac{(z^2(p \cdot q))}{N}}$$

n= Tamaño de la muestra

Z= Nivel de confianza deseado

p= Proporción de la población con la característica deseada (éxito)

q= Proporción de la población sin la característica deseada (fracaso)

e= Nivel de error dispuesto a cometer

N= Tamaño de la población

Muestreo:

La técnica estadística utilizada para la obtención de la muestra fue la no probabilística, porque “la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o los propósitos del investigador” (Hernandez, Fernandez & Baptista)

IV.4. Procedimientos, técnicas e instrumentos de recolección de información.

- **Procedimiento:**

Esta investigación se inició con una exposición detallada y una narración de la problemática actual, respaldada por trabajos previos y antecedentes relevantes. Para lograr una comprensión más profunda, se abordaron las teorías relacionadas con cada una de las variables bajo estudio, utilizando fuentes de información que en lo posible no superaran los 5 años de antigüedad, a menos que se tratara de teorías establecidas previamente.

Posteriormente, se delinearon los objetivos de investigación, se proporcionaron justificaciones sólidas que respaldaran el propósito de la

investigación y se establecieron hipótesis específicas para guiar el proceso. Se detalló la metodología que se seguiría, se definieron la población y la muestra que serían consideradas, y se procedió a la operacionalización de las variables, lo que incluyó la elaboración de los instrumentos necesarios para la técnica de la encuesta, entre otros aspectos metodológicos clave.

Además, se recopilaron datos de manera imparcial y sin adulteración alguna durante el proceso. Estos datos fueron sometidos a un riguroso proceso de análisis y procesamiento para obtener resultados precisos. A continuación, se presentaron estos resultados en la sección de discusión, donde se llevaron a cabo análisis profundos y se realizaron comparaciones relevantes. Las conclusiones de la investigación se derivaron de manera coherente a partir de los resultados obtenidos y se ofrecieron recomendaciones fundamentadas en base a los hallazgos.

Finalmente, como parte integral de este estudio, se propuso una solución a la problemática identificada. En resumen, esta investigación siguió un enfoque sistemático y riguroso desde el planteamiento del problema hasta la propuesta de solución, y se basó en evidencia actualizada para lograr resultados sólidos y significativos

- **Técnica de recolección de datos:**

En el marco de esta investigación, se optó por la aplicación de la técnica de recolección de datos conocida como encuesta. Esta metodología se define como un recurso valioso en el ámbito de la investigación de mercados, que se emplea para obtener información relevante de individuos que comparten características

similares. El procedimiento se lleva a cabo mediante la formulación de interrogantes diseñadas de acuerdo a indicadores previamente establecidos, tal y como se describe en el presente estudio de. A través de esta técnica, se busca obtener una visión más clara y precisa de las percepciones, opiniones o comportamientos de un grupo específico de personas, lo que proporciona datos esenciales para el análisis y la toma de decisiones en el contexto de la investigación.

- **Instrumentos para recolección de datos:**

En el curso de esta investigación, se empleó el instrumento del cuestionario para la obtención de datos directos de las unidades de análisis. Este instrumento, conocido como cuestionario de preguntas, desempeñó un papel fundamental en la recopilación de información esencial. Según la definición adoptada, un cuestionario se concibe como un documento en el cual se formulan un conjunto de preguntas específicas, las cuales se relacionan con los indicadores que requieren medición, y estas preguntas se vinculan estrechamente con las variables de estudio, tomando como base las dimensiones que guían la investigación. Es esencial destacar que cada una de estas preguntas debe guardar una estrecha relación con la formulación de los problemas de investigación y las hipótesis planteadas, asegurando así su relevancia en el contexto del estudio (Hernández, Fernández & Baptista, 2014).

En el contexto de esta investigación, los cuestionarios utilizados se estructuraron de manera minuciosa, con un total de 12 ítems para abordar las tres dimensiones relacionadas con la primera variable de estudio y 16 ítems para explorar las cuatro dimensiones vinculadas a la segunda variable. Estos ítems

se presentaron de manera que los participantes pudieran expresar sus respuestas mediante una escala politómica que comprende las opciones de Nunca (1), Casi nunca (2), A veces (3), Casi siempre (4) y Siempre (5). Estas respuestas politómicas se detallan en la escala de Likert, proporcionando una gama de opciones que permiten una evaluación más precisa de las actitudes y percepciones de los participantes en relación con los temas abordados en el cuestionario. La disposición y formulación de estos ítems se encuentran detalladas en el Anexo N°6: Instrumentos de recolección de datos, que acompaña a este estudio.

- **Validez y confiabilidad de los instrumentos:**

La investigación inicio con la descripción detallada de la problemática en cuestión, respaldada por investigaciones previas y antecedentes relevantes. Las teorías relacionadas con cada una de las variables bajo estudio se exploraron exhaustivamente, utilizando fuentes de información principalmente actualizadas en un período no superior a cinco años, con la excepción de aquellas teorías ya establecidas.

Posteriormente, se delinearon los objetivos de la investigación, se proporcionaron las justificaciones pertinentes y se formularon las hipótesis que servirían como guía en el desarrollo del estudio. Se estableció una metodología detallada que incluyó la identificación de la población y la selección de la muestra, además de la operacionalización de las variables clave y la creación de instrumentos específicos, como encuestas, diseñados para recopilar datos significativos.

En el proceso de recopilación de datos, se garantizó la integridad y la ausencia de cualquier tipo de manipulación, con el objetivo de obtener resultados veraces. Estos resultados se analizaron y discutieron en profundidad, lo que llevó a la formulación de conclusiones sólidas basadas en la evidencia recopilada. Además, se presentaron recomendaciones fundamentadas en los hallazgos, y se propuso una solución adecuada para abordar la problemática identificada. La investigación siguió un enfoque riguroso y metodológico desde la identificación del problema hasta la presentación de conclusiones y propuestas de solución, asegurando la validez y la integridad de los resultados obtenidos a lo largo de todo el proceso.

IV.5. Análisis estadístico

Antes de proceder con la recopilación y organización de datos, se realizó la codificación de la información en una matriz de tabulación de doble entrada, empleando la herramienta Software Office Excel 2022. Posteriormente, estos datos fueron transferidos al software especializado en estadística conocido como Statistical Package for the Social Sciences (SPSS) en la versión 26.

Una vez en el SPSS, se llevó a cabo un análisis exhaustivo de los resultados a través del enfoque de la estadística descriptiva. Se calcularon las frecuencias relativas y simples, proporcionando una visión detallada de la distribución de los datos. Estos resultados se presentaron de manera clara y accesible en tablas bidimensionales, facilitando un análisis descriptivo completo. Este análisis se enriqueció aún más con tablas cruzadas de frecuencia, que permitieron la observación de relaciones y patrones entre las variables pertinentes.

El enfoque del análisis no se detuvo ahí, ya que se tuvo en cuenta tanto los objetivos planteados como las hipótesis a evaluar. Para llevar a cabo un análisis inferencial significativo, se implementó una prueba de hipótesis. En este contexto, se optó por una prueba no paramétrica, y se utilizó el coeficiente RHO de Spearman. Esta elección estratégica permitió explorar y cuantificar la correlación existente entre las variables propuestas de una manera rigurosa y efectiva. Cabe indicar que el proceso de recolección, codificación, análisis y evaluación de datos se desarrolló con meticulosidad y rigor. Los resultados se presentaron de manera que permitieran un entendimiento claro y profundo de la información, y se utilizaron herramientas estadísticas especializadas para revelar relaciones y correlaciones relevantes. Este enfoque integral proporcionó una base sólida para la toma de decisiones informadas y el logro de los objetivos establecidos

Aspectos Éticos:

En el transcurso de la presente investigación, se ha mantenido un firme compromiso con la salvaguarda de la confidencialidad de los datos recolectados, así como con el respeto absoluto a las opiniones expresadas por los individuos participantes a través de los cuestionarios. Cabe destacar que el procesamiento de esta información ha sido ejecutado de manera rigurosa, garantizando que no se haya producido ninguna alteración o modificación indebida en los resultados obtenidos.

Adicionalmente, se ha prestado especial atención a la integridad académica y la correcta atribución de fuentes utilizadas durante el proceso de investigación. En este sentido, se ha seguido una meticulosa práctica de citación

y referencia bibliográfica, lo que contribuye a establecer un sólido fundamento para la investigación. Se ha otorgado un lugar fundamental al uso apropiado de las citas, reconociendo la autoría de las fuentes consultadas de acuerdo con los estándares académicos y éticos.

La integridad y originalidad de la investigación han sido salvaguardadas a través de la implementación de la herramienta Turnitin, reconocida por su capacidad para detectar el plagio y corroborar que el contenido de la investigación sea genuino y auténtico. Este recurso desempeña un papel esencial en garantizar la transparencia y la fiabilidad de los hallazgos obtenidos durante el curso de esta indagación.

En síntesis, se ha llevado a cabo una investigación rigurosa y ética, respetando la privacidad de los datos, la veracidad de las opiniones de los participantes y la originalidad de la obra. Además, se ha dado la debida importancia a la correcta atribución de fuentes, promoviendo la honestidad académica y el uso responsable de la información. La incorporación de Turnitin como herramienta anti-plagio contribuye a consolidar la integridad y legitimidad de este estudio.

V. RESULTADOS

V.1. Presentación y análisis de resultados

El análisis de frecuencias y porcentajes en relación con la variable de protección de datos personales y su vinculación con los derechos digitales proporciona una visión cuantitativa de la prevalencia y la interacción de estos elementos dentro del conjunto de datos examinado.

En términos de frecuencias, se trata de un desglose detallado de cuántas veces aparece una determinada categoría o respuesta en relación con la protección de datos personales y los derechos digitales. Los porcentajes, por otro lado, proporcionan una medida relativa al expresar estas frecuencias como una proporción del total. Esto puede ser particularmente útil al comparar diferentes subgrupos o categorías dentro de la variable en cuestión. Este análisis podrá revelar qué porcentaje de la muestra tiene una percepción positiva o negativa sobre la relación entre la protección de datos personales y los derechos digitales.

Este tipo de análisis estadístico es valioso para identificar patrones, tendencias o disparidades en la percepción o actitud hacia la protección de datos y los derechos digitales. Puede ayudar a comprender cómo estas dos variables están interconectadas en la mente de la población estudiada, y si existe alguna variación significativa en estas percepciones en función de ciertos factores demográficos u otros criterios de segmentación.

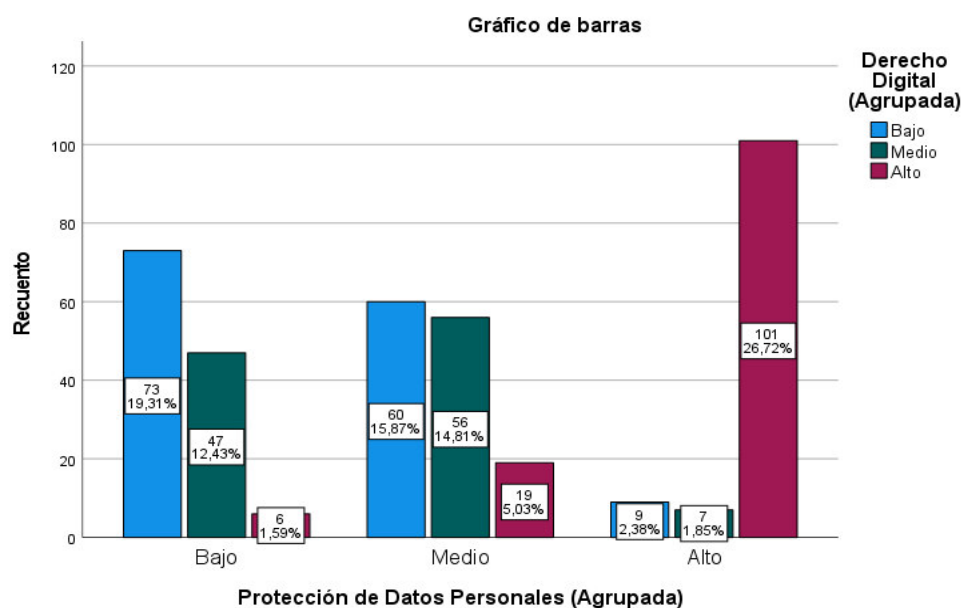
Tabla 1

Niveles de frecuencia y porcentajes sobre la Protección de los datos personales y los derechos digitales

			Derecho Digital			
			Bajo	Medio	Alto	Total
Protección de Datos Personales	Bajo	Recuento	73	47	6	126
		% del total	19,3%	12,4%	1,6%	33,3%
	Medio	Recuento	60	56	19	135
		% del total	15,9%	14,8%	5,0%	35,7%
	Alto	Recuento	9	7	101	117
		% del total	2,4%	1,9%	26,7%	31,0%
Total	Recuento	142	110	126	378	
	% del total	37,6%	29,1%	33,3%	100,0%	

Figura 1

Protección de los datos personales y los derechos digitales

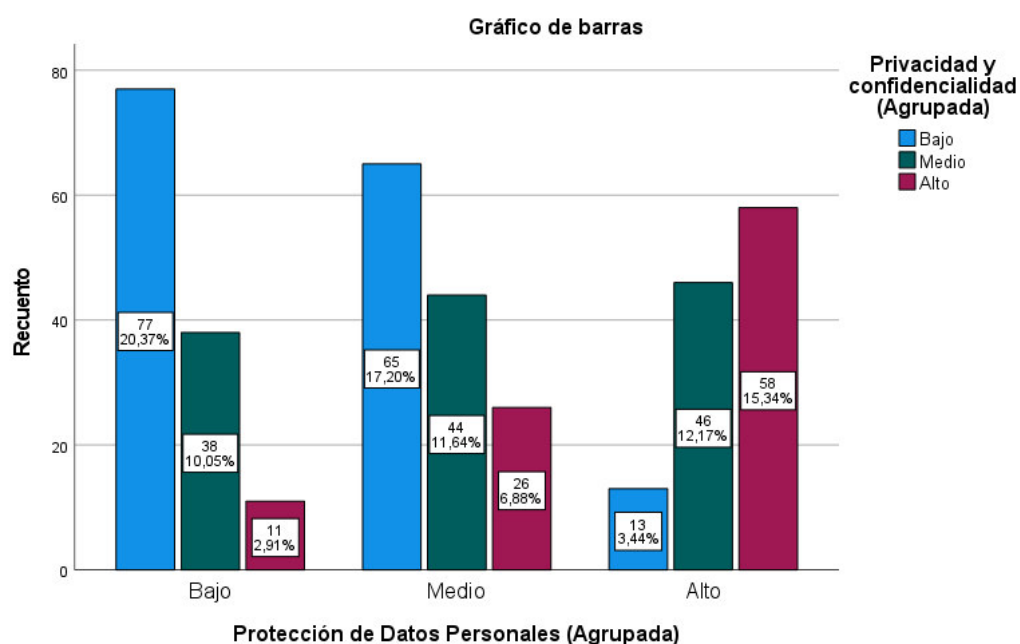


Interpretación

De la figura y tabla se aprecian los resultados generales de la percepción de los encuestados sobre los derechos digitales respecto a la protección de datos personales de donde se aprecia que el 37.60% considera que es bajo, el 29.10% que el nivel es medio y el 33.30% el señaló que es alta.

Tabla 2*Niveles de frecuencia y porcentajes sobre la Privacidad y confidencialidad*

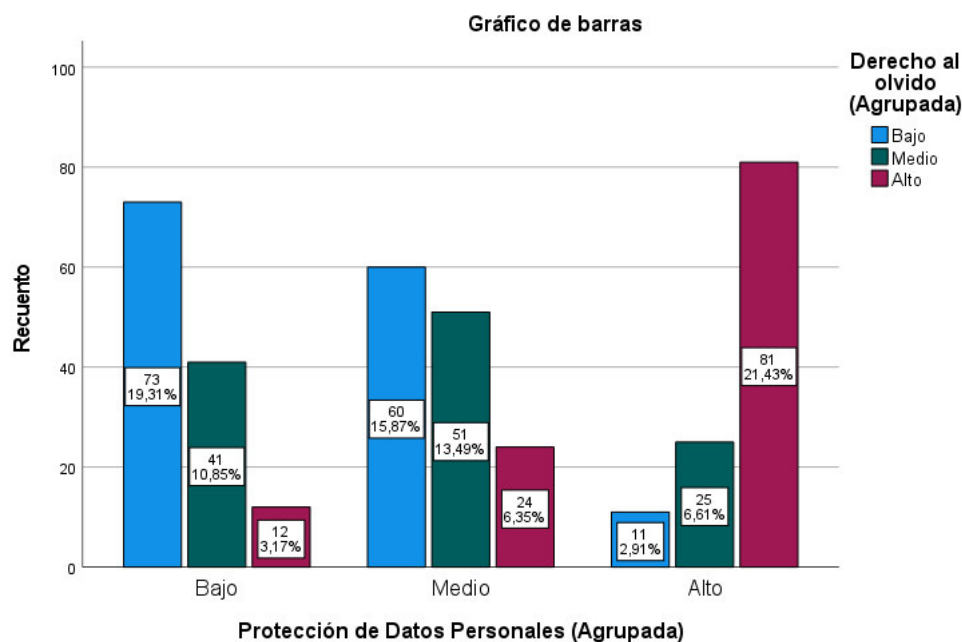
			Privacidad y confidencialidad			
			Bajo	Medio	Alto	Total
Protección de Datos Personales	Bajo	Recuento	77	38	11	126
		% del total	20,4%	10,1%	2,9%	33,3%
	Medio	Recuento	65	44	26	135
		% del total	17,2%	11,6%	6,9%	35,7%
	Alto	Recuento	13	46	58	117
		% del total	3,4%	12,2%	15,3%	31,0%
Total	Recuento	155	128	95	378	
	% del total	41,0%	33,9%	25,1%	100,0%	

Figura 2*Percepción sobre la Privacidad y confidencialidad***Interpretación**

De la figura y tabla se aprecian los resultados generales de la percepción de los encuestados sobre los privacidad y confidencialidad respecto a la protección de datos personales de donde se aprecia que el 41.00% considera que es bajo, el 33.90% que el nivel es medio y el 25.10% el señaló que es alta.

Tabla 3*Niveles de frecuencia y porcentajes sobre el derecho al olvido*

			Derecho al olvido			
			Bajo	Medio	Alto	Total
Protección de Datos Personales	Bajo	Recuento	73	41	12	126
		% del total	19,3%	10,8%	3,2%	33,3%
	Medio	Recuento	60	51	24	135
		% del total	15,9%	13,5%	6,3%	35,7%
	Alto	Recuento	11	25	81	117
		% del total	2,9%	6,6%	21,4%	31,0%
Total	Recuento	144	117	117	378	
	% del total	38,1%	31,0%	31,0%	100,0%	

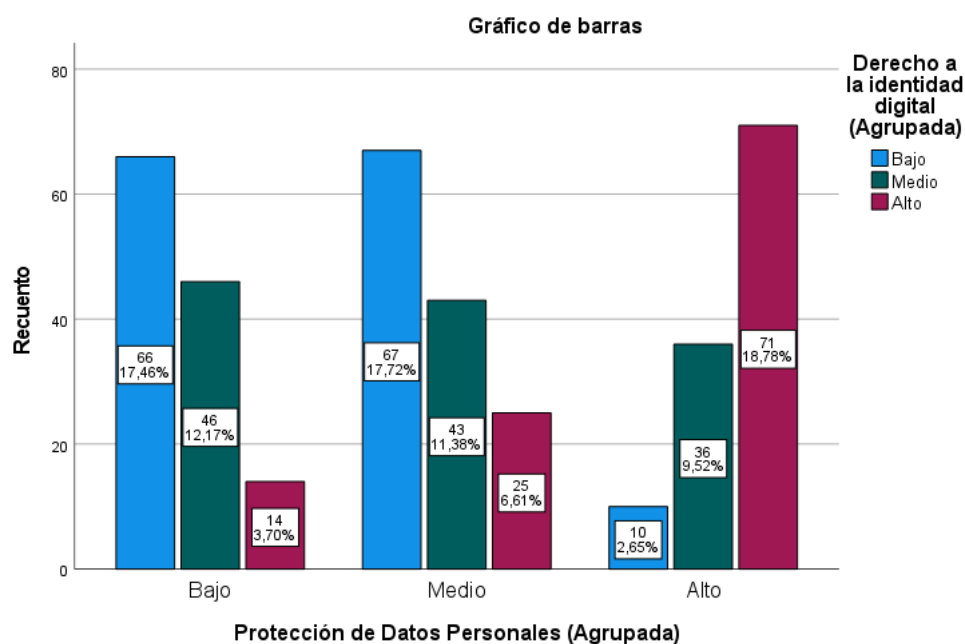
Figura 3*Percepción sobre el derecho al olvido*

Interpretación

De la figura y tabla se aprecian los resultados generales de la percepción de los encuestados sobre el derecho al olvido respecto a la protección de datos personales de donde se aprecia que el 38.10% considera que es bajo, el 31.00% que el nivel es medio y el 31.00% el señaló que es alta.

Tabla 4*Niveles de frecuencia y porcentajes sobre el derecho a la identidad digital*

			Derecho a la identidad digital			
			Bajo	Medio	Alto	Total
Protección de Datos Personales	Bajo	Recuento	66	46	14	126
		% del total	17,5%	12,2%	3,7%	33,3%
	Medio	Recuento	67	43	25	135
		% del total	17,7%	11,4%	6,6%	35,7%
	Alto	Recuento	10	36	71	117
		% del total	2,6%	9,5%	18,8%	31,0%
Total	Recuento	143	125	110	378	
	% del total	37,8%	33,1%	29,1%	100,0%	

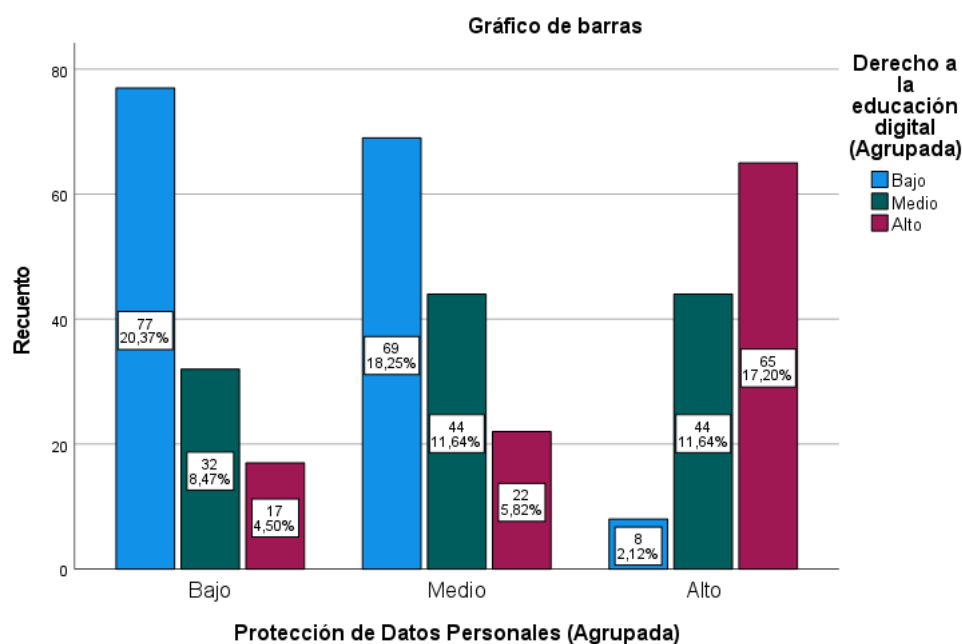
Figura 4*Percepción sobre el derecho a la identidad digital*

Interpretación

De la figura y tabla se aprecian los resultados generales de la percepción de los encuestados sobre los Derecho a la identidad digital respecto a la protección de datos personales de donde se aprecia que el 37.80% considera que es bajo, el 33.10% que el nivel es medio y el 29.10% el señaló que es alta.

Tabla 5*Niveles de frecuencia y porcentajes sobre el derecho a la educación digital*

			Derecho a la educación digital			
			Bajo	Medio	Alto	Total
Protección de Datos Personales	Bajo	Recuento	77	32	17	126
		% del total	20,4%	8,5%	4,5%	33,3%
	Medio	Recuento	69	44	22	135
		% del total	18,3%	11,6%	5,8%	35,7%
	Alto	Recuento	8	44	65	117
		% del total	2,1%	11,6%	17,2%	31,0%
Total	Recuento	154	120	104	378	
	% del total	40,7%	31,7%	27,5%	100,0%	

Figura 5*Percepción sobre el derecho a la educación digital*

Interpretación

De la figura y tabla se aprecian los resultados generales de la percepción de los encuestados sobre la educación digital respecto a la protección de datos personales de donde se aprecia que el 40.7% considera que es bajo, el 31.70% que el nivel es medio y el 27.50% el señaló que es alta.

Contrastación de hipótesis general y específica

Hipótesis general

H0: No Existe relación entre la protección de datos y los derechos digitales en el Perú

H1: Existe relación entre la protección de datos y los derechos digitales en el Perú

Tabla 6

Coefficiente de Correlación de Rho de Spearman de Protección de datos personales y Derechos digitales

			Protección de Datos Personales	Derecho Digital
Rho de Spearman	Protección de Datos Personales	Coefficiente de correlación	1,000	,615**
		Sig. (bilateral)	.	,000
		N	378	378
	Derecho Digital	Coefficiente de correlación	,615**	1,000
		Sig. (bilateral)	,000	.
		N	378	378

** . La correlación es significativa en el nivel 0,01 (bilateral).

El coeficiente de Rho de Spearman resultó con un valor de 0.615, lo que nos indica que existe una correlación positiva directa del tipo moderada, esta correlación es significativa a un nivel de 0,01 (1%). Por otra parte, el nivel de significancia bilateral fue menor a 0,05 ($0,0000 < 0,01$), esto implica rechazar la hipótesis nula y aceptar la hipótesis alternativa, es decir que los derechos digitales se relacionan moderadamente con la protección de datos en el Perú.

Hipótesis específica 1

H0: No existe la relación entre la protección de datos personales y la Privacidad y confidencialidad digital en el Perú

H1: Existe la relación entre la protección de datos personales y la Privacidad y confidencialidad digital en el Perú

Tabla 7

Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Privacidad y confidencialidad

			Protección de Datos Personales	Privacidad y confidencialidad
Rho de Spearman	Protección de Datos Personales	Coeficiente de correlación	1,000	,452**
		Sig. (bilateral)	.	,000
		N	378	378
	Privacidad y confidencialidad	Coeficiente de correlación	,452**	1,000
		Sig. (bilateral)	,000	.
		N	378	378

** . La correlación es significativa en el nivel 0,01 (bilateral).

El coeficiente de Rho de Spearman resultó con un valor de 0.452, lo que nos indica que existe una correlación positiva directa del tipo moderada, esta correlación es significativa a un nivel de 0,01 (1%). Por otra parte, el nivel de significancia bilateral fue menor a 0,05 ($0,0000 < 0,01$), esto implica rechazar la hipótesis nula y aceptar la hipótesis alternativa, es decir que la Privacidad y confidencialidad digital se relaciona moderadamente con la protección de datos en el Perú.

Hipótesis específica 2

H0: No existe la relación entre la protección de datos personales y el derecho al olvido digital en el Perú

H1: Existe la relación entre la protección de datos personales y el derecho al olvido digital en el Perú

Tabla 8

Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derecho al olvido

			Protección de Datos Personales	Derecho al olvido
Rho de Spearman	Protección de Datos Personales	Coeficiente de correlación	1,000	,514**
		Sig. (bilateral)	.	,000
		N	378	378
	Derecho al olvido	Coeficiente de correlación	,514**	1,000
		Sig. (bilateral)	,000	.
		N	378	378

**. La correlación es significativa en el nivel 0,01 (bilateral).

El coeficiente de Rho de Spearman resultó con un valor de 0.514, lo que nos indica que existe una correlación positiva directa del tipo moderada, esta correlación es significativa a un nivel de 0,01 (1%). Por otra parte, el nivel de significancia bilateral fue menor a 0,05 ($0,0000 < 0,01$), esto implica rechazar la hipótesis nula y aceptar la hipótesis alternativa, es decir que el derecho al olvido digital se relaciona moderadamente con la protección de datos en el Perú.

Hipótesis específica 3

H0: No existe la relación entre la protección de datos personales y el Derecho a la identidad digital en el Perú

H1: Existe la relación entre la protección de datos personales y el Derecho a la identidad digital en el Perú

Tabla 9

Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derecho a la identidad digital

			Protección de Datos Personales	Derecho a la identidad digital
Rho de Spearman	Protección de Datos Personales	Coeficiente de correlación	1,000	,393**
		Sig. (bilateral)	.	,000
		N	378	378
	Derecho a la identidad digital	Coeficiente de correlación	,393**	1,000
		Sig. (bilateral)	,000	.
		N	378	378

** . La correlación es significativa en el nivel 0,01 (bilateral).

El coeficiente de Rho de Spearman resultó con un valor de 0.393, lo que nos indica que existe una correlación positiva directa del tipo baja, esta correlación es significativa a un nivel de 0,01 (1%). Por otra parte, el nivel de significancia bilateral fue menor a 0,05 ($0,0000 < 0.01$), esto implica rechazar la hipótesis nula y aceptar la hipótesis alternativa, es decir que el derecho a la identidad digital se relaciona de manera baja con la protección de datos en el Perú.

Hipótesis específica 4

H0: No existe la relación entre la protección de datos personales y el Derecho a la educación digital en el Perú

H1: Existe la relación entre la protección de datos personales y el Derecho a la educación digital en el Perú

Tabla 10

Coeficiente de Correlación de Rho de Spearman de Protección de datos personales y Derecho a la educación digital

			Protección de Datos Personales	Derecho a la educación digital
Rho de Spearman	Protección de Datos Personales	Coeficiente de correlación	1,000	,376**
		Sig. (bilateral)	.	,000
		N	378	378
	Derecho a la educación digital	Coeficiente de correlación	,376**	1,000
		Sig. (bilateral)	,000	.
		N	378	378

** . La correlación es significativa en el nivel 0,01 (bilateral).

El coeficiente de Rho de Spearman resultó con un valor de 0.376, lo que nos indica que existe una correlación positiva directa del tipo baja, esta correlación es significativa a un nivel de 0,01 (1%). Por otra parte, el nivel de significancia bilateral fue menor a 0,05 ($0,0000 < 0.01$), esto implica rechazar la hipótesis nula y aceptar la hipótesis alternativa, es decir que el derecho a la educación digital se relaciona de manera baja con la protección de datos en el Perú.

VI. DISCUSIÓN

En relación a la **hipótesis general** que postula "Existe relación entre la protección de datos personales y los derechos digitales en el Perú", el investigador Salinas & Vasquez, (2023) respalda de manera contundente dicha afirmación a través de su investigación. Identifica un conflicto palpable entre el derecho a la protección de datos personales y el derecho a la intimidad en una entidad de salud, destacando la compleja intersección de estos dos aspectos. La falta de cumplimiento subraya la imperante necesidad de fortalecer la conexión entre las políticas internas y los requisitos legales. Además, las propuestas de mejora no solo buscan corregir deficiencias, sino también establecer un precedente valioso para otras organizaciones, contribuyendo así a la promoción de los derechos digitales, especialmente en el ámbito de la salud.

Por otro lado, el investigador Huerta & Cochachin, (2021) respalda significativamente la hipótesis general. Destaca el derecho al olvido digital como un componente esencial para equilibrar la libertad de información y la protección de datos personales, estableciendo así una conexión directa entre la protección de datos y los derechos digitales. La regulación de la difusión de información personal en internet, basada en criterios legales, pone de relieve la interdependencia crucial entre la protección de datos y el respeto a los derechos digitales en el contexto peruano. Lo que coincide con lo señalado por Luna Cervantes (2021) quien postula la existencia de una conexión intrínseca entre la protección de datos y los derechos digitales en el contexto peruano. Su investigación proporciona una base sólida para evaluar esta hipótesis, abordando de manera integral las dinámicas y desafíos relacionados con la

protección de datos en Perú. Destaca la relevancia de esta hipótesis al señalar que la falta de protección de datos puede amenazar directamente los derechos digitales, como la privacidad y la confidencialidad.

Cabe indicar que Revoredo-Palacios (2021), al explorar la publicidad programática, revela una intersección crítica entre el uso de datos personales y la protección de la privacidad en el entorno digital, respaldando así la hipótesis general. Sugiere que la protección de datos personales es intrínseca para salvaguardar los derechos digitales en el contexto peruano.

Por otro lado Saavedra-Grados (2023), al revelar una vulneración significativa de datos personales y el incumplimiento generalizado de la Ley de Protección de Datos Personales, destaca la urgencia de mejorar la aplicación de la ley para garantizar la protección de la privacidad. Este escenario subraya la interdependencia entre la regulación de protección de datos y la efectividad de los derechos digitales. A esto se suma lo señalado por Rudas Chara & Carpio Romero (2020) que evidencian claramente que la protección de datos está directamente vinculada a los derechos digitales. La vulneración significativa al derecho a la privacidad como lo sucedido a los usuarios del Banco de Crédito y subraya la importancia de una protección efectiva de datos para preservar los derechos digitales fundamentales.

Es importante destacar lo señalado por Lombarte (2020) que subraya la importancia de la relación entre los derechos digitales y las políticas estatales. La diversidad de estrategias observadas en los tres países estudiados destaca que la protección de datos y los derechos digitales están intrínsecamente vinculados a las decisiones gubernamentales y a las respuestas específicas a

situaciones críticas. Esto se alinea con lo señalado por Barrio (2021) plantea que se debe garantizar la seguridad y privacidad de los datos como fundamental para el ejercicio pleno de los derechos digitales, y este merece un análisis detallado. Asimismo comparte lo señalado por Moreno-Bobadilla, quien destacó que la conexión intrínseca entre el derecho al olvido digital y la protección de datos en la investigación europea, anticipando que esta relación es crucial en el contexto peruano. La evolución del derecho al olvido digital en Europa destaca la necesidad de marcos legales adaptables para salvaguardar la privacidad y la autonomía en un entorno digital.

Se debe tomar en consideración lo señalado por Segura (2019) arroja luz sobre la compleja dinámica del activismo por los derechos digitales en América Latina. Este contexto puede extrapolarse al Perú, evidenciando que la protección de datos está intrínsecamente ligada a los derechos digitales. La diversidad de actores involucrados destaca la necesidad de una comprensión integral en la relación entre la protección de datos y los derechos digitales. La conclusión de que la región está inmersa en la construcción de nuevos marcos interpretativos relacionados con los derechos digitales refuerza la hipótesis general al subrayar que la evolución constante de la tecnología digital requiere una adaptación continua de políticas y estrategias.

Por otro lado (2020) Roca reafirma que la evolución del derecho a la protección de datos es esencial para adaptarse a los cambios tecnológicos, respaldando así la hipótesis general. La legislación europea ha respondido activamente a los desafíos digitales, y este enfoque podría proporcionar lecciones valiosas para fortalecer los derechos digitales en el contexto peruano.

En ese sentido Castellanos-Claramunt (2020), proporciona un sólido respaldo a la hipótesis general al destacar las complejas interconexiones entre la gestión de datos y los derechos digitales. La conclusión de que la gestión de la información en la era digital va más allá de lo legal para abarcar profundas implicaciones éticas y sociales respalda la noción de que la protección de datos está intrínsecamente vinculada a la salvaguarda de los derechos fundamentales en el entorno digital. Este enfoque multidisciplinario subraya la necesidad de considerar no solo aspectos legales sino también éticos al desarrollar políticas y prácticas relacionadas con la protección de datos en el Perú. Lo cual es refrendado por Vázquez-Cano & Pascual-Moscoso (2022) que aportan valiosa información para respaldar la investigación, revelando que el conocimiento y la aplicación ética de la tecnología en la educación son cruciales. La protección de datos personales se convierte en un componente fundamental de esta relación, ya que la carencia de conocimientos por parte del profesorado en los protocolos y normas de uso de dispositivos y programas informáticos resalta la necesidad urgente de intervenciones formativas.

En relación con la **hipótesis específica 01**, que establece la existencia de una conexión entre la protección de datos personales y la privacidad y confidencialidad digital en el Perú, diversos investigadores han aportado valiosa información respaldando dicha hipótesis.

El investigador Salinas & Vasquez, (2023) afirma que la investigación respalda directamente esta hipótesis específica. La falta de cumplimiento de la ley de protección de datos personales en una entidad de salud revela una vulneración significativa de la privacidad y confidencialidad digital. La brecha

entre las políticas internas y los requisitos legales indica una falta de salvaguardias adecuadas para proteger la información personal, evidenciando la necesidad de una conexión más fuerte entre estas dos esferas. Es así como Huerta & Cochachin, (2021), sostienen que la investigación respalda la hipótesis específica 01 al centrarse en el derecho al olvido digital, limitando la difusión indiscriminada de datos personales en línea. La protección de datos personales no solo es crucial para preservar la privacidad, sino también para salvaguardar la confidencialidad en el entorno digital. Luna Cervantes, (2021) destaca que la investigación se centra en la privacidad y confidencialidad digital, fortaleciendo la conexión con la hipótesis específica 01. La relevancia de esta relación se manifiesta en conclusiones que destacan dinámicas y desafíos relacionados con la protección de datos, siendo la privacidad uno de los aspectos más cruciales. La relación directa entre la protección de datos y la privacidad es esencial para garantizar un entorno digital seguro y confiable.

No debemos dejar de pasar por alto lo señalado por Revoredo-Palacios (2021), quien subraya cómo la publicidad programática depende fuertemente del uso de datos personales, resaltando desafíos significativos en términos de protección de la privacidad. Esta relación directa respalda la hipótesis específica 01, mostrando que la protección de datos es esencial para preservar la privacidad y confidencialidad digital en el Perú. Saavedra-Grados (2023), destaca la vulneración significativa de datos personales, especialmente por parte de empresas privadas. Este hallazgo refuerza la idea de que la protección de datos es fundamental para preservar la privacidad y confidencialidad digital. La necesidad de abordar la debilidad en la aplicación de la ley resalta la importancia de fortalecer la protección de datos para garantizar la privacidad en el entorno

digital peruano. Mismo sentir de Rudas Chara & Carpio Romero (2022) quienes sostienen que la afectación al derecho a la privacidad de los usuarios del sector bancario y como se debe tener en consideración la relación intrínseca entre la protección de datos y la privacidad digital. La inadecuada salvaguarda de la información personal evidencia una brecha en la confidencialidad digital.

Lombarte (2020) sugiere que la atención a la privacidad y la confidencialidad digital muestra la relación fundamental entre la protección de datos y estos aspectos críticos. En el contexto peruano, la implementación de políticas estatales y estrategias empresariales podría tener un impacto directo en la privacidad y confidencialidad digital de los ciudadanos. Es por ello como lo señala Barrio (2021) destaca la urgencia de abordar la transición de la era analógica a la digital y señala la falta de un entorno de seguridad jurídica en esta transformación. La relación entre la protección de datos y la privacidad digital es evidente, ya que la protección efectiva de datos es esencial para preservar la privacidad y confidencialidad de los individuos en el entorno digital. La legislación vigente, similar a la Ley Orgánica 3/2018 en España, puede ofrecer un marco, pero la eficacia depende de su implementación y adaptación a la realidad peruana. Eso es reforzado por lo señalado por Moreno-Bobadilla (2020), quien sostiene que la investigación europea demuestra que el derecho al olvido digital está estrechamente vinculado a la privacidad. Este vínculo sugiere que la protección de datos es esencial para preservar la privacidad y confidencialidad digital que debe aplicarse en el contexto peruano. La implementación efectiva de medidas de protección de datos puede ser crucial para garantizar la privacidad en el espacio digital.

Por otro lado, Segura (2019), reafirma que la complejidad en la formulación de políticas y estrategias destaca que la protección de datos está directamente vinculada a la privacidad y confidencialidad en la era digital. Los desafíos específicos en América Latina subrayan la necesidad de políticas que aborden la gestión de datos para resguardar la privacidad de los ciudadanos. Es por lo que Roca (2020), destaca la importancia del consentimiento del interesado. La privacidad y la confidencialidad digital están intrínsecamente vinculadas a cómo se manejan y protegen los datos personales. La legislación peruana podría beneficiarse al revisar y fortalecer las disposiciones relacionadas con el consentimiento.

Se debe también destacar que Castellanos-Claramunt (2020), sostiene que la investigación que destaca la importancia de considerar tanto aspectos éticos como jurídicos al implementar sistemas de inteligencia artificial respalda la hipótesis específica 01. La privacidad y confidencialidad digital son elementos fundamentales afectados por la gestión de datos en la era digital. La necesidad de salvaguardar estos aspectos se evidencia en la emergencia de nuevos derechos, como el derecho al olvido. Vázquez-Cano & Pascual-Moscoso confirman la hipótesis específica 01 al señalar que el uso poco sostenible de dispositivos digitales puede tener impactos psicoemocionales en los estudiantes. Subrayan la conexión entre la protección de datos y la privacidad digital, indicando que los protocolos de protección son elementos fundamentales para el bienestar psicológico de los usuarios.

En relación con la **hipótesis específica 02**, que establece la existencia de una relación entre la protección de datos personales y el derecho al olvido

digital en el Perú, diversos investigadores han proporcionado valiosas perspectivas que respaldan esta conexión. Por ello que Salinas & Vasquez, (2023) indican que, aunque en su investigación no abordaron directamente el derecho al olvido digital, la propuesta de alternativas para fortalecer la ley y mejorar la implementación puede considerarse como un paso hacia el reconocimiento y aplicación de este derecho. La necesidad de corregir deficiencias identificadas sugiere la importancia de permitir que la información obsoleta o no relevante se retire del ámbito digital, respaldando así la conexión entre la protección de datos y el derecho al olvido. Esto se sustenta por lo indicado por Huerta & Cochachin, (2021), quienes sostienen por su parte que la investigación demuestra cómo el derecho al olvido digital es una manifestación práctica de la protección de datos personales en el contexto peruano. Limitar la difusión de información personal en línea constituye un componente esencial de la protección de datos y, por ende, respalda la relación propuesta.

Lo señalado se suma a lo indicado por Luna Cervantes, (2021) destaca que el enfoque general en la protección de datos proporciona un marco relevante. La conexión entre la protección de datos y el derecho al olvido es evidente, ya que ambos están relacionados con el control sobre la información personal en línea. La efectividad de las políticas y prácticas existentes puede influir directamente en la capacidad de ejercer el derecho al olvido. Revoredo-Palacios (2021), aunque no aborda directamente el derecho al olvido digital, señala que la discusión sobre la necesidad de salvaguardar la privacidad en la publicidad programática se vincula indirectamente. Esto sugiere que la protección de datos es crucial para respaldar el derecho al olvido digital, ya que ambos están enraizados en la gestión ética de la información personal. De la

misma manera Saavedra-Grados (2023), que tampoco abordó directamente el derecho al olvido, la vulneración de datos personales y el impacto negativo significativo resaltan la importancia de considerar este derecho. La persistencia de información personal de manera no regulada puede tener consecuencias negativas, lo que sugiere la necesidad de medidas para implementar el derecho al olvido y equilibrar la protección de datos.

Es así que Rudas Chara & Carpio Romero (2022), sostienen que el uso incorrecto de la información y la falta de mecanismos efectivos de control señalan la importancia del derecho al olvido digital. La investigación sugiere la necesidad de considerar cómo la protección de datos puede respaldar este derecho en el entorno digital peruano. Por otro lado, Lombarte (2020) destaca que la atención al derecho al olvido digital en la investigación de Huerta & Gabriela (2021), refuerza la hipótesis específica 02. La interconexión entre la protección de datos y el derecho al olvido destaca la necesidad de políticas y prácticas que permitan a las personas controlar la permanencia de su información en línea. En esta línea Barrio menciona que aunque la investigación no aborda directamente el derecho al olvido digital, considerando el contexto general de la protección de datos y derechos digitales, se puede argumentar que el derecho al olvido es esencial en la preservación de la privacidad. Este derecho asegura que la información obsoleta o irrelevante no siga afectando negativamente a las personas en el entorno digital.

También se debe destacar que Moreno-Bobadilla (2020), se centró en el derecho al olvido digital, evidenciando su complejidad y evolución. Extrapolando estos resultados al Perú, se puede esperar que la protección de datos esté

directamente relacionada con el derecho al olvido digital. Una legislación sólida en protección de datos puede ser la base para garantizar la implementación efectiva del derecho al olvido. Por ello Segura (2019), sostiene que el reconocimiento de elementos novedosos entrelazados con problemas históricos respalda la hipótesis específica 02. La conclusión de que la región está construyendo nuevos marcos interpretativos sugiere que el derecho al olvido digital es una herramienta esencial en esta reevaluación constante de demandas y estrategias en la protección de datos. Igual conclusión a la que llega Roca (2020), destaca la adaptación activa de la jurisprudencia europea, señalada por la investigación, sugiere la importancia de revisar y actualizar las regulaciones en respuesta a la evolución tecnológica. Esto respalda la idea de que el derecho al olvido digital debería ser considerado y adaptado en la legislación peruana para abordar la perennidad de la información en línea.

Asimismo, Castellanos-Claramunt (2020), valida directamente la hipótesis específica 02 al identificar el derecho al olvido como uno de los nuevos derechos que emergen de la necesidad de proteger los datos personales en el contexto de la inteligencia artificial. Este derecho es crucial para equilibrar el poder de la información en un entorno digital donde la persistencia indefinida de datos puede tener consecuencias significativas en la privacidad y otros derechos digitales. A esto se suma lo indicado por Vázquez-Cano & Pascual-Moscoso (2022), quienes señalan la relevancia de la ética en el uso de la tecnología en la educación sugiere una conexión en este sentido. La necesidad de abordar preocupaciones psicoemocionales resalta la importancia de manejar la información de manera ética y segura, contribuyendo indirectamente al derecho al olvido digital.

En relación con la **hipótesis específica 03**, que postula la existencia de una relación entre la protección de datos personales y el derecho a la identidad digital en el Perú, diversos investigadores han aportado análisis esclarecedores que respaldan esta conexión. A este respecto Salinas & Vasquez, (2023) sostienen que la falta de cumplimiento de la ley tiene implicaciones directas en el derecho a la identidad digital. La mala aplicación de la ley y la brecha entre las políticas internas y los requisitos legales podrían conducir a la manipulación o mal uso de la información personal, afectando la integridad de la identidad digital de los individuos. Por ello Saavedra-Grados (2023), señala una debilidad en los órganos competentes encargados de hacer cumplir la ley, lo que contribuye a la falta de aplicación efectiva de las disposiciones legales y permite la vulneración de datos. Esto destaca la relevancia de fortalecer la protección de datos para preservar la identidad digital de los individuos en el contexto peruano. Esto refuerza lo indicado por Rudas Chara & Carpio Romero (2022), quienes mencionan que debe haber una mayor concientización sobre la normativa de protección de datos. Esto es crucial para fortalecer la identidad digital, ya que la correcta gestión de los datos personales es esencial para preservar la integridad de la identidad digital.

Cabe indicar que Huerta & Cochachin, (2021) y Lombarte (2020), indican que la identidad digital se constituye en una limitación de la difusión de información personal en línea y se puede considerar un elemento crucial para preservar la integridad de la identidad digital. La capacidad de controlar la presencia en línea contribuye indirectamente a la protección de la identidad digital. Luna Cervantes, (2021) también destaca que respecto el derecho a la identidad digital, la naturaleza reflexiva de su enfoque implica una consideración

amplia de las cuestiones clave relacionadas con la protección de datos. La conexión entre la protección de datos y la identidad digital se deriva de la importancia de asegurar que la información personal no sea mal utilizada, lo que puede afectar la identidad digital de las personas. Por ello Revoredo-Palacios (2021), resalta la importancia de comprender cómo se abordan los desafíos en la protección de datos en el contexto de la publicidad programática. Esta comprensión es esencial para respaldar la hipótesis específica 03, ya que la identidad digital está intrínsecamente ligada a la forma en que se manejan los datos personales en el entorno digital.

Por otro Barrio (2021), destaca que el derecho a la identidad digital implica proteger la integridad y autenticidad de la información personal en línea. La investigación destaca la importancia de los derechos digitales en el nuevo paradigma digital, lo que sugiere una conexión inherente con la protección de la identidad digital. La legislación futura podría incluir disposiciones específicas para salvaguardar este derecho. Por ello Moreno-Bobadilla señala la importancia de la identidad digital. Por eso en el Perú, la protección de datos puede ser esencial para preservar la identidad digital de las personas, especialmente en un entorno digital en constante evolución. Lo que refuerza lo señalado por Segura (2019), destaca la construcción de nuevos marcos interpretativos implica una constante reevaluación de cómo se aborda la identidad digital, respaldando así la hipótesis específica 03. En esta misma línea Roca (2020), sugiere que el análisis comparativo entre corrientes anglosajona y germana del derecho a la protección de datos debe proporcionar una perspectiva valiosa sobre cómo diferentes enfoques pueden impactar la identidad digital. Esta hipótesis podría

explorar cómo la legislación peruana puede aprender de estas corrientes para fortalecer el derecho a la identidad digital.

En relación con la **hipótesis específica 04**, que plantea la existencia de una relación entre la protección de datos personales y el derecho a la educación digital en el Perú, distintos investigadores han proporcionado análisis fundamentados que respaldan esta interconexión. Luna Cervantes, (2021) sostiene que la relación entre la protección de datos y el derecho a la educación digital encuentra apoyo en la investigación. Al abordar las áreas de mejora y las consideraciones éticas en juego, la investigación destaca la necesidad de concientización y comprensión sobre la importancia de la protección de datos. Esta conciencia es esencial para la educación digital efectiva. Por ello Salinas & Vasquez, (2023) señalan que la educación digital y la falta de cumplimiento identificada sugiere la necesidad de una mayor conciencia y comprensión de la ley de protección de datos personales. Esto puede interpretarse como una llamada de atención para mejorar la educación digital en organizaciones de salud, destacando la relación entre la protección de datos y el conocimiento adecuado de los derechos digitales.

Lo señalado por Huerta & Cochachin, (2021) es importante debido al hecho que destacan la importancia de implementar medidas que limiten la perennidad de la información en línea para proteger la privacidad y los derechos digitales. Este enfoque podría considerarse parte integral de la educación digital, ya que promueve la conciencia sobre la gestión responsable de la información personal en el entorno digital. Lo que refrenda lo señalado por Revoredo-Palacios (2021), aunque no aborda directamente la educación digital, centra su

atención en las prácticas de recopilación y uso de datos personales en la publicidad programática, resaltando la importancia de la conciencia y la comprensión en este ámbito. Esto respalda la hipótesis específica 04, sugiriendo que una sólida protección de datos contribuirá a un entorno educativo digital más seguro y de esta manera generar un ámbito de protección del consumidor el cual brinda sus datos personales para su custodia y buen uso.

En ese sentido Saavedra-Grados (2023), identifica la generación de conocimiento y la concienciación como aspectos cruciales. La investigación no solo revela problemas específicos en la protección de datos en las organizaciones, sino que también destaca la necesidad de intervenciones efectivas. Esto sugiere la importancia de la educación digital como parte integral de las medidas para mejorar la protección de datos y fortalecer los derechos digitales. Cabe indicar al respecto que Rudas Chara & Carpio Romero (2022), destacan la necesidad de difundir y promover el cumplimiento de las normas de protección de datos. Esto resalta la relevancia de la educación en este ámbito y cómo el conocimiento más amplio sobre la Ley Nro. 29733 que contribuye a la creación de una cultura de respeto a la privacidad digital. Por ello Moreno-Bobadilla (2020) destaca la complejidad del derecho al olvido digital en la era digital y resalta la necesidad de educación digital. La protección de datos puede ser fundamental para empoderar a los ciudadanos con conocimientos sobre cómo proteger su privacidad en línea, respaldando así la hipótesis de la relación con la educación digital.

Se tiene una coincidencia resaltante con Lombarte (2020), que subraya la importancia de la educación digital en la sociedad actual, destacando la

necesidad de abordar la relación entre la protección de datos y este derecho. La forma en que se protegen los datos puede afectar la calidad y el alcance de la educación digital disponible para los ciudadanos peruanos. Por ello se debe tomar en consideración lo señalado por Barrio (2021) quien apunta hacia la posibilidad de un nuevo orden jurisdiccional adaptado a los asuntos digitales. Esto podría implicar una consideración especial para el derecho a la educación digital, ya que un orden jurisdiccional adaptado podría facilitar la implementación de programas educativos robustos para mejorar la alfabetización digital y la conciencia sobre la protección de datos. Lo señalado se refuerza con lo indicado por Segura (2019) que concluye que los desafíos específicos en América Latina relacionados con el acceso, producción y gestión digital y de datos respaldan la hipótesis específica 04. Además señala que la protección de datos es esencial para garantizar un entorno de educación digital seguro y ético, y la investigación destaca que estos desafíos deben abordarse de manera específica en el contexto latinoamericano.

Apartado aparte merece lo referido por Roca (2020) quien enfatiza la importancia de la educación digital como marco normativo del cualquier estado moderno, resaltando la necesidad de educación y concienciación sobre la protección de datos. La legislación peruana podría integrar medidas que promuevan la educación digital para empoderar a los ciudadanos en el manejo seguro de sus datos. Lo que refuerza lo señalado por Castellanos (2020) quien destaca resalta la relevancia de abordar cuestiones como la automatización de decisiones y el uso de datos en ámbitos críticos como la educación. La protección de datos está directamente relacionada con la forma en que se utilizan los datos en contextos educativos, y la consideración ética y legal es esencial

para garantizar el respeto de los derechos digitales de los individuos. Por otro lado a esto se debe sumar lo indicado por Vázquez-Cano & Pascual-Moscoso (2022) quienes subrayan la falta de conocimientos sobre los protocolos y normas de uso de dispositivos y programas informáticos, reforzando la necesidad de un enfoque pedagógico que integre prácticas éticas y seguras. Esta integración es esencial para garantizar no solo la protección de datos sino también para avanzar en el derecho a la educación digital.

El conjunto de conclusiones extraídas de diversas fuentes investigativas se configura un panorama integral y esclarecedor en relación con la confluencia de la protección de datos y los derechos digitales en el contexto peruano. La diversidad de las perspectivas contempladas refleja la intrincada naturaleza de estos asuntos fundamentales en la era digital (Berdote, 2022). No obstante, es pertinente señalar ciertos aspectos que podrían enriquecer aún más la comprensión integral.

En primer lugar, la noción de la diversidad de contextos emerge como un elemento clave. Aunque la atención se centra en nuestra capital, Lima, sería invaluable desplegar un análisis más minucioso sobre cómo las realidades particulares de diversas regiones o sectores, ya sea el ámbito de la salud, la educación, el sector financiero, entre otros, podrían ejercer una influencia singular entre la protección de datos y los derechos digitales. Este enfoque permitiría una comprensión más precisa y contextualizada de los desafíos y oportunidades presentes en cada esfera.

El énfasis en soluciones prácticas, señalado como un segundo punto, se erige como una necesidad apremiante. Mientras las conclusiones subrayan la

importancia de políticas y prácticas efectivas, existe un espacio para una mayor profundización en propuestas concretas (Duque, 2019). La identificación de soluciones específicas no solo conferiría un carácter más aplicable a las recomendaciones sino también fortalecería la eficacia de las medidas propuestas.

Al proyectar la mirada hacia el futuro, el reconocimiento y abordaje de posibles desafíos emergentes constituye el tercer punto crucial. La veloz evolución tecnológica introduce constantes desafíos, y una perspectiva proactiva es esencial para anticipar y mitigar posibles riesgos (Ibarra, 2023). Explorar este aspecto aportaría una visión más completa y robusta entre la protección de datos y los derechos digitales.

Finalmente, la consideración de factores culturales, como se sugiere en el cuarto punto, añadiría una dimensión enriquecedora al análisis. En un país tan diverso culturalmente como Perú, entender cómo las percepciones culturales influyen en la percepción y abordaje de la protección de datos y los derechos digitales podría proporcionar discernimientos valiosos. Esto no solo complementarían el análisis general sino que también podría informar estrategias más contextualizadas y efectivas.

Los diferentes estudios de estos investigadores proporcionan una visión integral y enriquecedora sobre la intersección entre la protección de datos y los derechos digitales en el contexto peruano, destacando la relación contundente entre ambas esferas. Se identifica un conflicto tangible entre el derecho a la protección de datos y el derecho a la intimidad en todo ámbito del que hacer humano, subrayando la urgencia de fortalecer la conexión entre las políticas

internas y los requisitos legales. Las propuestas de mejoras no solo apuntan a corregir deficiencias, sino también a establecer un precedente valioso para otras organizaciones, contribuyendo así a la promoción de los derechos digitales, especialmente en el ámbito de la gestión organizacional.

Las investigaciones respaldan significativamente la hipótesis general, haciendo hincapié en el derecho al olvido digital como un componente esencial para equilibrar la libertad de información y la protección de datos personales. Existe una conexión directa entre la protección de datos y los derechos digitales, focalizándose en la regulación de la difusión de información personal en internet basada en criterios legales. Esta conexión intrínseca entre la protección de datos y los derechos digitales se refuerza con la investigación que aborda de manera integral las dinámicas y desafíos relacionados con la protección de datos en Perú.

La exploración de la publicidad programática respalda la hipótesis general al revelar una intersección crítica entre el uso de datos personales y la protección de la privacidad en el entorno digital. Se sugiere que la protección de datos personales es intrínseca para salvaguardar los derechos digitales en el contexto peruano. Además, se destaca la urgencia de mejorar la aplicación de la ley para garantizar la protección de la privacidad, revelando una vulneración significativa de datos personales y el incumplimiento generalizado de la Ley de Protección de Datos Personales.

Se evidencia que la protección de datos está directamente vinculada a los derechos digitales, subrayando la importancia de una protección efectiva de datos para preservar los derechos digitales fundamentales. Asimismo, se

destaca la importancia de la relación entre los derechos digitales y las políticas estatales, enfatizando que la protección de datos y los derechos digitales están intrínsecamente vinculados a las decisiones gubernamentales.

La necesidad de garantizar la seguridad y privacidad de los datos como fundamentales para el ejercicio pleno de los derechos digitales se plantea con firmeza. Se subraya la conexión intrínseca entre el derecho al olvido digital y la protección de datos en la investigación europea, anticipando que esta relación es crucial en el contexto peruano.

Estas investigaciones arrojan luz sobre la compleja dinámica del activismo por los derechos digitales en América Latina, evidenciando que la protección de datos está intrínsecamente ligada a los derechos digitales. Se demuestra que la evolución del derecho a la protección de datos es esencial para adaptarse a los cambios tecnológicos, respaldando así la hipótesis general. Castellanos Claramunt proporciona un sólido respaldo a la hipótesis general al destacar las complejas interconexiones entre la gestión de datos y los derechos digitales.

Las investigaciones aportan valiosa información respaldando las hipótesis planteadas, revelando que el conocimiento y la aplicación ética de la tecnología en la educación son cruciales. La protección de datos personales se convierte en un componente fundamental de esta relación, destacando la necesidad urgente de intervenciones formativas. En conjunto, estos análisis convergen en respaldar la hipótesis general sobre la relación entre la protección de datos y los derechos digitales en el contexto peruano. En este contexto, es crucial considerar la legislación peruana y su alineación con los estándares

internacionales en materia de derechos digitales y protección de datos personales.

Cabe indicar que como parte de la una política clara de protección de datos relacionados a los derechos digitales se tiene que fortalecer en la práctica Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) que son fundamentales en materia de protección de datos, tanto a nivel nacional como internacional, y su inclusión en la legislación peruana refleja un avance significativo en la salvaguardia de los derechos digitales de los ciudadanos, sin embargo se debe monitorizar y supervisar su cumplimiento por las organizaciones sean estas público o privadas.

En el contexto peruano, la incorporación de los derechos ARCO en la legislación ha fortalecido la posición de los individuos respecto al manejo de sus datos personales. El derecho de Acceso permite a las personas conocer qué información se está recopilando y procesando sobre ellas, fomentando la transparencia por parte de las entidades que manejan datos. La Rectificación y Cancelación aseguran que los individuos puedan corregir información incorrecta o desactualizada, y solicitar la eliminación de sus datos cuando ya no sean necesarios para la finalidad original. Por último, el derecho de Oposición permite a las personas manifestar su negativa al tratamiento de ciertos datos, especialmente en situaciones donde el consentimiento es fundamental.

Desde una perspectiva internacional, estos derechos se alinean con principios clave de protección de datos presentes en normativas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esto

es crucial no solo para la interoperabilidad en un mundo interconectado, sino también para la protección de los ciudadanos peruanos en contextos globales.

La relevancia de los derechos ARCO a nivel internacional se manifiesta en la promoción de estándares comunes que resguardan la privacidad y empoderan a los individuos en relación con sus datos personales. Esto no solo facilita la libre circulación de datos entre diferentes jurisdicciones, sino que también fomenta un entorno global en el que la protección de datos es un derecho universal.

Sin embargo, es fundamental reconocer que la implementación efectiva de estos derechos depende no solo de su inclusión en la legislación, sino también de la capacidad de las autoridades y las entidades relevantes para garantizar su cumplimiento. Además, en un entorno digital en constante evolución, es crucial revisar y actualizar estas disposiciones para abordar nuevos desafíos y tecnologías emergentes. La presencia de los derechos ARCO en la legislación peruana no solo es esencial para proteger los derechos digitales de los ciudadanos a nivel nacional, sino que también contribuye a la convergencia con estándares internacionales, fortaleciendo así la posición de Perú en el escenario global de protección de datos.

VII. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Primera

Los hallazgos de esta investigación revelan una correlación significativa entre la protección de datos personales y los derechos digitales en el contexto peruano. Estos derechos digitales, que abarcan aspectos clave como la privacidad y otros derechos fundamentales en el entorno digital, se ven influidos de manera considerable por las políticas y regulaciones de protección de datos implementadas en el país. Esta conexión directa destaca la importancia crítica de establecer y mantener un marco legal robusto que salvaguarde la integridad y privacidad de los datos personales en el ámbito digital.

La validación de la hipótesis se ha llevado a cabo mediante un análisis estadístico inferencial, específicamente a través del coeficiente de correlación de Rho Spearman. El valor obtenido, que asciende a 0,615, indica una relación moderada entre las variables objeto de estudio. Este resultado estadístico refuerza y respalda la conclusión de que, efectivamente, existe una conexión sustancial entre la protección de datos personales y la garantía de derechos digitales en el contexto peruano.

La correlación moderada sugiere que las variaciones en la protección de datos personales tienden a estar asociadas con cambios correspondientes en la preservación y respeto de los derechos digitales. Es decir, un fortalecimiento en las políticas de protección de datos se asocia positivamente con una mayor protección y promoción de los derechos digitales en el entorno peruano.

Estos resultados no solo validan la hipótesis inicial de la investigación, sino que también ofrecen una base estadística sólida para respaldar las conclusiones cualitativas. La relación significativa identificada implica que cualquier mejora en la protección de datos personales puede tener un impacto directo y positivo en la salvaguarda de los derechos digitales en el Perú. En consecuencia, estos hallazgos no solo informan sobre la conexión intrínseca entre ellas, sino que también subrayan la importancia de intervenciones y políticas específicas para fortalecer ambas dimensiones en conjunto.

Segunda

Los resultados de nuestro estudio brindan un respaldo sustancial a la hipótesis que postula la existencia de una conexión significativa entre la protección de datos personales y la privacidad y confidencialidad digital en el contexto peruano. Este respaldo no se basa únicamente en observaciones cualitativas, sino que se refuerza con un análisis estadístico inferencial, en particular, mediante el cálculo del coeficiente de correlación de Spearman, que arrojó un valor de 0.452.

Este coeficiente de correlación, al ser positivo y mayor que cero, indica una relación moderada entre las variables objeto de estudio. En este caso, la protección de datos personales y la privacidad y confidencialidad digital están vinculadas de manera significativa. La magnitud del coeficiente sugiere que, a medida que aumenta la protección de datos, hay una tendencia correlativa a mejorar la privacidad en línea y la confidencialidad de la información personal en el contexto digital peruano.

El papel crucial de las políticas de protección de datos en esta interrelación destaca la importancia de un marco normativo sólido y efectivo. Estas políticas no solo sirven como salvaguarda legal para los individuos en términos de cómo se manejan y protegen sus datos, y también contribuyen directamente a la preservación de la privacidad en línea. La privacidad y confidencialidad de la información personal son aspectos cruciales en un entorno digital donde la recopilación y el intercambio de datos son necesarias.

Es importante destacar que, al establecer esta relación, no solo se evidencia la importancia de la protección de datos para la privacidad individual, sino también para la confianza general en los entornos digitales. La confidencialidad de la información personal es esencial para fomentar un ambiente en línea donde los usuarios se sientan seguros y protegidos, lo que, a su vez, impulsa la participación activa y el aprovechamiento pleno de las oportunidades digitales.

Sin embargo, aunque nuestra investigación ha identificado una relación moderada, es fundamental reconocer que esta relación es dinámica y sujeta a cambios en el tiempo y en respuesta a los avances tecnológicos y cambios en las prácticas de gestión de datos. Por lo tanto, la adaptabilidad de las políticas y regulaciones de protección de datos se vuelve crucial para mantener la relevancia y la efectividad en un entorno digital en constante evolución.

Tercera

La investigación revela un hallazgo significativo al confirmar la existencia de una relación sustancial entre la protección de datos personales y el derecho al olvido

digital en el contexto peruano. Este vínculo se sustenta en las regulaciones de protección de datos que, al ser implementadas adecuadamente, proporcionan el marco legal necesario para la aplicación efectiva del derecho al olvido digital. Este derecho otorga a los individuos el poder de solicitar la eliminación de información personal en línea, bajo condiciones específicas y justificadas.

La relación cuantificada estadísticamente a través de un valor de Rho Spearman de 0.514 revela una correlación moderada entre las variables estudiadas. Este resultado fortalece la validez de la hipótesis planteada, indicando que a medida que se fortalece la protección de datos personales, también se potencia la aplicación del derecho al olvido digital en el entorno digital peruano.

La moderada correlación sugiere que, si bien existe una relación significativa entre estas dos variables, no se trata de una conexión extrema ni absoluta. La implementación eficaz del derecho al olvido está influida por varios factores, incluida la robustez de las leyes de protección de datos, la conciencia pública sobre estos derechos y la capacidad de las plataformas en línea para responder a tales solicitudes.

Este hecho tiene implicaciones profundas, ya que resalta la importancia de contar con marcos legales sólidos y efectivos para la protección de datos personales. La capacidad de las personas para controlar y gestionar la información que circula sobre ellas en línea se convierte en un componente esencial de la protección de su privacidad y, por ende, de sus derechos digitales.

Además, la presencia de una relación moderada subraya la necesidad de un enfoque equilibrado en la formulación de políticas. No solo es crucial fortalecer las leyes de protección de datos, sino también educar a la población sobre sus derechos digitales y fomentar la responsabilidad por parte de las entidades que manejan datos.

Cuarta

Los hallazgos de nuestra investigación proporcionan una sólida base para respaldar la hipótesis de que la protección de datos personales está intrínsecamente relacionada con el derecho a la identidad digital en el contexto peruano. Este respaldo se fundamenta en la evidencia de que las leyes de protección de datos desempeñan un papel crucial en la salvaguarda de la identidad digital de las personas y en la mitigación del riesgo de uso no autorizado de datos personales.

La relación entre la protección de datos y la identidad digital se ha explorado a través de un análisis estadístico inferencial, utilizando el coeficiente de correlación de Spearman (Rho Spearman). Los resultados revelan un valor de 0.393, indicando una relación baja pero significativa entre las variables objeto de estudio. Este valor numérico proporciona una medida cuantitativa de la conexión entre la protección de datos personales y el derecho a la identidad digital.

La relación baja sugiere que, aunque hay una asociación, esta no es de fuerza intensa. Sin embargo, este tipo de relación no debe subestimarse, ya que incluso una conexión moderada puede tener implicaciones significativas en la

preservación de la identidad digital de los individuos. Este resultado estadístico respalda la idea de que las regulaciones de protección de datos desempeñan un papel relevante, aunque quizás no totalmente determinante, en la configuración y salvaguarda de la identidad digital en el contexto específico del Perú.

Quinta

La investigación revela de manera contundente la existencia de una relación de relevancia entre dos aspectos críticos en la sociedad peruana contemporánea: la protección de datos personales y el acceso al derecho a la educación digital. Este hallazgo sugiere que las políticas y prácticas orientadas a salvaguardar la seguridad y privacidad de los datos de los usuarios desempeñan un papel crucial en facilitar un acceso efectivo a la educación digital en el país.

La conexión entre la protección de datos y la educación digital tiene implicaciones significativas en un mundo cada vez más digitalizado. La consideración de la seguridad y privacidad de la información personal se vuelve esencial para fomentar la confianza de los usuarios y, por ende, para promover la participación efectiva en entornos educativos digitales. Los individuos son más propensos a participar activamente en plataformas de educación digital si tienen la certeza de que sus datos personales están protegidos de manera adecuada.

El valor de Rho Spearman de 0,376, obtenido a través del análisis estadístico inferencial, indica una relación baja pero significativa entre las variables en estudio. Aunque la correlación no es alta, la estadística muestra una asociación que refuerza la hipótesis inicial. Este valor sugiere que, a medida que se fortalecen las políticas de protección de datos, existe un aumento modesto

pero estadísticamente significativo en el acceso al derecho a la educación digital. Es fundamental considerar que la baja correlación no implica una relación débil; más bien, destaca la multifactorialidad de los elementos que influyen en la relación entre estas variables.

La protección de datos personales en el contexto de la educación digital puede abordar preocupaciones legítimas sobre la privacidad de los ciudadanos, la integridad de la información y la confianza en las plataformas tanto públicas como privadas. Asimismo, estos resultados respaldan la noción de que la seguridad y privacidad son componentes esenciales para crear un entorno propicio para el aprendizaje digital.

Es crucial destacar que, si bien la relación es evidente, la dirección precisa de la causalidad no se establece claramente a través de este análisis. Podría ser que un acceso mejorado a la educación digital motive un mayor interés en la protección de datos, o viceversa. Este aspecto podría ser objeto de investigaciones futuras para comprender más a fondo la dinámica de esta relación.

Recomendaciones

Primera

Se recomienda que el estado peruano deba fortalecer y mejorar el marco legal de protección de datos en el ámbito gubernamental, esto es crucial para salvaguardar los derechos digitales y la privacidad de los ciudadanos en el entorno digital en constante evolución. Para implementar esta recomendación de manera efectiva, se pueden proponer las siguientes mejoras organizacionales:

Revisión y Actualización Continua: Es fundamental establecer un mecanismo de revisión y actualización periódica de la legislación existente. Esto implica una respuesta ágil a los cambios tecnológicos y las dinámicas emergentes en el tratamiento de datos personales. La creación de un equipo especializado encargado de monitorear las tendencias y revisar la legislación contribuiría a mantenerla relevante y efectiva.

En primer lugar, se debe alinear la legislación con estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, con ello se fortalecerá la posición de Perú en el escenario global y se facilitará la transferencia segura de datos con otras jurisdicciones. Establecer un grupo de trabajo para analizar y adoptar prácticas y estándares internacionales sería beneficioso.

En segundo lugar, se debe fomentar la transparencia en la elaboración de políticas relacionadas con la protección de datos que es una tarea esencial. La inclusión de la ciudadanía en el proceso mediante consultas públicas y

participación ciudadana contribuirá a la creación de leyes más equitativas y a la aceptación general de las medidas implementadas.

En tercer lugar, se debe reforzar los órganos de supervisión encargados de garantizar el cumplimiento de las leyes de protección de datos. Esto implica proporcionar recursos adecuados y capacitación especializada a estas entidades para que puedan llevar a cabo auditorías efectivas y hacer cumplir las regulaciones de manera proactiva.

En cuarto lugar, se deben introducir incentivos para que las empresas y organizaciones adopten buenas prácticas en protección de datos. Esto puede incluir beneficios fiscales, reconocimientos públicos o certificaciones que demuestren el cumplimiento de estándares de privacidad.

En quinto lugar, se debe establecer mecanismos de coordinación efectivos entre diferentes entidades gubernamentales para garantizar una aplicación coherente de las leyes de protección de datos. La colaboración entre los ministerios pertinentes y las instituciones responsables fortalecerá la aplicación y supervisión de las normativas.

En sexto lugar, se debe implementar sistemas de cumplimiento proactivo, como auditorías regulares y revisiones de impacto en la privacidad, para garantizar que las organizaciones estén cumpliendo con las leyes de protección de datos. Establecer consecuencias claras para el incumplimiento ayudará a disuadir prácticas no éticas.

La implementación de estas mejoras organizacionales no solo robustecerá el marco legal de protección de datos en Perú, sino que también

contribuirá a construir una cultura de respeto a la privacidad y conciencia digital en la sociedad.

Segunda

Se recomienda que las autoridades peruanas intensifiquen sus esfuerzos para fomentar la conciencia y la educación en torno a la protección de datos personales. La promoción de campañas de educación pública y la implementación de programas de formación exhaustivos, tanto en entornos escolares como empresariales, constituyen estrategias cruciales para empoderar a los ciudadanos y fortalecer la protección de datos en el país.

En primer lugar, se sugiere que las autoridades diseñen y ejecuten campañas de educación pública que aborden de manera clara y accesible los conceptos fundamentales de la protección de datos personales. Estas campañas podrían incluir material informativo en diversos formatos, como anuncios televisivos, publicaciones en redes sociales, carteles y folletos distribuidos en lugares clave. Además, se podría considerar la colaboración con instituciones educativas y organizaciones de la sociedad civil para amplificar el alcance de estas campañas.

Asimismo, en el entorno empresarial, se recomienda que las autoridades fomenten la implementación de programas de formación obligatorios para empleados en relación con las mejores prácticas de protección de datos. Estos programas podrían enfocarse en la seguridad de la información, el manejo ético de datos personales y la comprensión de las obligaciones legales en materia de

privacidad. Las empresas también podrían ser incentivadas a adoptar certificaciones de protección de datos como parte de sus prácticas estándar.

Para maximizar el impacto, se sugiere que estas iniciativas de concientización se desarrollen en colaboración con expertos en protección de datos, académicos y profesionales de la industria. Además, la inclusión de módulos de aprendizaje en línea podría proporcionar flexibilidad y accesibilidad a un público más amplio.

Tercera

Se recomienda la implementación efectiva del derecho a la eliminación de información personal en línea, también conocido como el derecho al olvido digital, es fundamental para garantizar una protección robusta de los derechos digitales en el contexto peruano. Para mejorar la organización y ejecución de este proceso.

Es esencial que las autoridades peruanas establezcan procedimientos claros y accesibles para que las personas ejerzan su derecho al olvido digital. Estos procedimientos deben ser comprensibles para el ciudadano común y fácilmente accesibles en línea. Se deberían proporcionar formularios y recursos en línea para facilitar el proceso de solicitud.

Por otro lado se debe implementar plataformas en línea dedicadas para la presentación de solicitudes de eliminación de información personal puede agilizar el proceso. Estas plataformas deberían ser seguras y fáciles de usar, permitiendo a los individuos presentar sus solicitudes de manera eficiente. La

plataforma también podría servir como un recurso educativo, proporcionando información detallada sobre el derecho al olvido y los pasos a seguir.

Las autoridades peruanas deben establecer mecanismos de cooperación efectiva con los proveedores de servicios en línea. Esto implica acordar pautas y procesos para la rápida eliminación de datos personales cuando se recibe una solicitud válida. La colaboración puede incluir la definición de estándares para la notificación oportuna a los solicitantes sobre la eliminación de datos.

Se debe lanzar campañas educativas para aumentar la conciencia sobre el derecho al olvido digital y cómo ejercerlo. Muchas personas pueden no estar al tanto de este derecho, y la información educativa puede empoderar a los ciudadanos para que tomen medidas para proteger su privacidad en línea.

También se debe definir plazos claros para el procesamiento de solicitudes y la eliminación de información personal. Esto brinda certeza a los solicitantes sobre cuándo pueden esperar que se tomen medidas. Además, plazos transparentes pueden ayudar a mantener la responsabilidad y la eficiencia en el proceso en todo tipo de organización.

Se debe Implementar un sistema de monitoreo continuo para evaluar la efectividad del proceso de eliminación de datos personales. Este monitoreo podría incluir la revisión de la velocidad de respuesta, el cumplimiento de plazos y la calidad de la comunicación con los solicitantes.

Demos buscar asegurar que los procedimientos implementados estén alineados con los estándares internacionales, como los establecidos por la Unión Europea en el Reglamento General de Protección de Datos (GDPR). Esto no

solo garantiza la coherencia a nivel global, sino que también facilita la transferencia segura de datos entre jurisdicciones.

Se debe incluir como mecanismo incluir a la sociedad civil en la formulación y revisión de políticas relacionadas con el derecho al olvido. Esto asegura la representación de diversas perspectivas y experiencias, fortaleciendo así la legitimidad del proceso.

Al implementar estas mejoras organizacionales, las autoridades peruanas pueden crear un entorno más eficiente y transparente para el ejercicio del derecho al olvido digital, promoviendo una protección más efectiva de los derechos digitales de los ciudadanos.

Cuarta

Se recomienda que tanto las instituciones gubernamentales como las entidades privadas refuercen de manera significativa la seguridad en la gestión de la identidad digital. La actualización y mejora de los sistemas de autenticación son fundamentales para mitigar riesgos asociados con el acceso no autorizado a datos personales, lo cual es esencial para la protección de la privacidad y la prevención de posibles usos indebidos.

Una mejora organizacional sugerida consiste en la implementación de sistemas de autenticación multifactorial. Este enfoque avanzado va más allá de la simple combinación de nombre de usuario y contraseña, incorporando capas adicionales de seguridad, como códigos temporales o biometría. Estas medidas no solo hacen más difícil el acceso no autorizado, sino que también proporcionan un nivel adicional de certeza sobre la identidad del usuario.

Además, se recomienda una revisión y fortalecimiento constante de las políticas de seguridad de la información en estas organizaciones. Esto implica la identificación y corrección proactiva de posibles vulnerabilidades en los sistemas, así como la implementación de medidas de seguridad robustas en todas las etapas del manejo de la identidad digital. La adopción de estándares de seguridad reconocidos a nivel internacional puede ser beneficiosa en este sentido.

La concienciación y capacitación continua del personal sobre prácticas seguras en la gestión de datos personales son elementos esenciales de cualquier estrategia de mejora organizacional. Esto no solo incluye al personal de tecnología de la información, sino a todos los empleados que manejan información sensible. La cultura de seguridad debe ser inculcada en toda la organización para garantizar la participación activa y consciente de todos los miembros.

Asimismo, se sugiere la implementación de herramientas de monitoreo avanzadas que permitan la detección temprana de posibles amenazas y actividades sospechosas. Los sistemas de alerta y respuesta rápida son esenciales para abordar cualquier incidente de seguridad de manera oportuna y reducir al mínimo los posibles impactos negativos.

Quinta

Se recomienda que las autoridades gubernamentales desplieguen estrategias integrales para fomentar el acceso a la educación digital con un enfoque específico en la promoción del respeto a la protección de los datos personales y

derechos digitales para todos los ciudadanos. Esta recomendación no solo abarca la inversión en infraestructura digital, sino también se extiende a la garantía de que se respeten rigurosamente las normas de privacidad y seguridad de datos de los ciudadanos, lo que puede llevar a mejoras significativas a nivel organizacional.

En primer lugar, la inversión en infraestructura digital debe ser planificada y ejecutada estratégicamente para garantizar un acceso equitativo a recursos educativos en línea. Esto implica la creación de programas de conectividad robustos que alcancen tanto áreas urbanas como rurales. Asimismo, se debe priorizar el acceso a dispositivos adecuados para la participación efectiva en la educación digital, asegurando que la brecha digital no excluya a ninguna población.

Paralelamente, es esencial desarrollar e implementar programas de formación continua para los ciudadanos sobre el uso responsable de la tecnología y la protección de datos personales. Estos programas podrían abordar temas como la importancia de contraseñas seguras, la conciencia sobre el manejo de la información personal en línea y la identificación de posibles amenazas cibernéticas. Integrar estas temáticas en el currículo educativo formal también podría ser beneficioso.

Para garantizar la efectividad de estas medidas, las normas de privacidad y seguridad de datos deben ser estrictamente cumplidas por todas las entidades, tanto públicas como privadas. Esto implica establecer mecanismos de supervisión y cumplimiento que aseguren que las organizaciones manejen los datos personales de los ciudadanos con el más alto grado de integridad y

seguridad. Estos mecanismos podrían incluir auditorías regulares y la imposición de sanciones significativas por violaciones a la privacidad.

Además, la transparencia en la recopilación y uso de datos debe ser un principio rector. Las organizaciones deben informar claramente a los ciudadanos sobre cómo se están utilizando sus datos y obtener su consentimiento informado. La educación digital también puede desempeñar un papel crucial en empoderar a los individuos para que comprendan y ejerzan sus derechos digitales, incluido el derecho a controlar sus datos personales.

VIII. PROPUESTA

Título: *“Propuesta para la creación de una norma legal que fortalezca la protección de datos personales y la identidad digital a través de la educación digital.”*

VIII.1. Introducción

La propuesta legislativa para impulsar la protección de datos personales y la identidad digital a través de la educación digital en el Perú se fundamenta en la creciente importancia de la tecnología en la sociedad actual. Esta propuesta busca asegurar que los ciudadanos posean las herramientas y conocimientos necesarios para salvaguardar su privacidad y derechos digitales.

Desde una perspectiva constitucional, la propuesta se alinea con la Constitución Política del Perú. Reconoce el derecho fundamental a la protección de datos personales, según el artículo 2, inciso 6, y considera el derecho a la educación, establecido en el artículo 13. En este contexto, la inclusión de la educación digital se presenta como un elemento integral de este derecho.

Los pilares fundamentales de la ley incluyen la obligatoriedad de la educación digital en todos los niveles educativos, con programas específicos que aborden la protección de datos, privacidad en línea y gestión de la identidad digital. Se propone la formación continua de docentes en el ámbito de la educación digital, promoviendo colaboraciones con expertos y organizaciones especializadas para desarrollar contenidos educativos actualizados y pertinentes.

La inclusión de temas específicos, como el manejo de contraseñas y la configuración de la privacidad en redes sociales, se destaca como una medida esencial. La propuesta también establece mecanismos de evaluación periódica para medir la efectividad de los programas y realizar ajustes según las necesidades cambiantes.

La justificación de la propuesta se basa en el empoderamiento ciudadano, proporcionando habilidades para tomar decisiones informadas sobre el manejo de datos personales. Asimismo, busca prevenir riesgos como el ciberacoso y la suplantación de identidad desde edades tempranas. En un contexto de rápida transformación digital, la propuesta apunta a garantizar que la población se adapte a nuevas dinámicas y comprenda los desafíos asociados a la protección de la identidad digital.

Además, la propuesta se alinea con estándares internacionales en materia de protección de datos y derechos digitales, fortaleciendo la posición del Perú en el ámbito global. En conclusión, la implementación de esta ley no solo asegurará la protección de datos personales y la identidad digital de los ciudadanos, sino que también contribuirá a formar una sociedad digitalmente competente y consciente de sus derechos y responsabilidades en el entorno digital.

VIII.2. Problemática

La creciente integración de la tecnología en la sociedad peruana ha dado paso a una serie de desafíos y problemáticas en torno a la protección de datos personales y la identidad digital. La falta de conocimientos específicos en estos ámbitos expone a los ciudadanos a riesgos significativos, como la pérdida de

privacidad, el robo de identidad y la exposición a actividades delictivas en línea. La brecha educativa en materia de tecnología y protección de datos se traduce en una vulnerabilidad generalizada de la población frente a las amenazas digitales.

VIII.3. Objetivos de la propuesta

a. Empoderamiento Ciudadano:

- El problema radica en la falta de conocimiento sobre la protección de datos personales deja a los ciudadanos indefensos ante posibles violaciones de privacidad.
- Por ello el objetivo es dotar a la población con conocimientos sólidos para que puedan ejercer un control efectivo sobre su información personal, empoderándolos para tomar decisiones informadas en entornos digitales.

b. Prevención de Riesgos:

- El problema radica en la ignorancia acerca de los riesgos digitales, como el ciberacoso y el robo de identidad, aumenta la exposición de la población a estas amenazas.
- Por ello el objetivo es implementar programas educativos que no solo informen sobre los riesgos, sino que también proporcionen estrategias y habilidades para prevenir y responder a situaciones de riesgo digital.

c. Adaptación a la Transformación Digital:

- El problema radica en la rápida evolución tecnológica supera la capacidad de adaptación de muchos ciudadanos, lo que resulta en una desconexión con las prácticas digitales más seguras.
- Por ello el objetivo es facilitar la adaptación de la población a las transformaciones digitales, asegurando que estén al tanto de los

desarrollos tecnológicos y comprendan las mejores prácticas para proteger sus datos en entornos en constante cambio.

d. Cumplimiento de Estándares Internacionales:

- El problema radica en la falta de regulación específica en torno a la protección de datos y la identidad digital puede dejar a Perú rezagado en términos de estándares internacionales.
- Por ello el objetivo es alinear la legislación peruana con los estándares internacionales, fortaleciendo así la posición del país en el ámbito global y facilitando la cooperación internacional en materia de protección de datos.

VIII.4. Análisis SEPTE

El análisis SEPTE es un enfoque metodológico que evalúa los impactos y consideraciones en cinco dimensiones principales: Socioeconómica, Ética, Política, Tecnológica y Ambiental. Este análisis se utiliza para comprender de manera integral las diversas implicaciones de una acción, decisión o propuesta en estas áreas clave. A continuación desarrollamos este análisis con la finalidad de darle sostenibilidad a la propuesta.

a. Socioeconómico:

La necesidad de la educación digital en el contexto de la protección de datos personales y la identidad digital en el Perú se refleja en aspectos socioeconómicos. Una población informada y capacitada en estos temas es más resistente a posibles amenazas cibernéticas, lo que puede contribuir a la estabilidad y confianza en el entorno digital. Además, ciudadanos educados digitalmente pueden participar de manera más activa y segura en

la economía digital, lo que tiene implicaciones positivas para el desarrollo económico.

b. Ético:

Desde la perspectiva ética, la educación digital se presenta como un imperativo para respetar los derechos individuales y la privacidad. La falta de conocimiento en estos temas puede resultar en prácticas digitales irresponsables o incluso en el abuso de la información personal. La educación digital, en este sentido, no solo es un medio para empoderar, sino también para inculcar valores éticos relacionados con el uso responsable de la tecnología.

c. Político:

En el ámbito político, la educación digital se vincula con la promoción de una ciudadanía más consciente y participativa. Ciudadanos informados sobre la protección de datos y la identidad digital pueden influir de manera más efectiva en las políticas relacionadas con la privacidad en línea. Además, la adopción de estándares internacionales en esta materia puede fortalecer la posición del país en la arena política global.

d. Tecnológico:

En el aspecto tecnológico, la educación digital es esencial para aprovechar al máximo las oportunidades ofrecidas por la transformación digital. La falta de conocimientos en protección de datos podría frenar la adopción de tecnologías emergentes. Una población educada en estos aspectos puede beneficiarse plenamente de las innovaciones digitales mientras minimiza los riesgos asociados.

e. Ambiental:

Desde un punto de vista ambiental, la educación digital puede contribuir a la sostenibilidad al promover prácticas digitales seguras y eficientes. Un entendimiento adecuado de la protección de datos y la identidad digital puede llevar a un uso más consciente de la tecnología, reduciendo así el impacto ambiental asociado con la gestión de grandes cantidades de datos

**VIII.5. Propuesta de Marco legal respecto a la Educación Digital y
Protección de Datos en el Perú - Exposición de Motivos**

En el contexto de la acelerada transformación digital de nuestra sociedad, la presente ley se erige como una respuesta proactiva y necesaria para abordar los desafíos emergentes en la convergencia de la tecnología y los derechos ciudadanos. Su propósito central es establecer una política pública integral de Educación Digital, enfocándose de manera especial en la protección de datos personales tanto en instituciones públicas como privadas en el territorio peruano.

La primera década del siglo XXI ha sido testigo de una revolución digital que ha transformado radicalmente la forma en que vivimos, trabajamos y nos relacionamos. La omnipresencia de la tecnología digital ha conllevado beneficios significativos, pero también ha generado desafíos inéditos en cuanto a la protección de derechos fundamentales, especialmente en lo que respecta a la privacidad y seguridad de los datos personales.

Es evidente que la creciente digitalización de la sociedad peruana ha traído consigo beneficios significativos, pero también ha planteado desafíos fundamentales en la protección de datos personales y los derechos digitales. En este contexto, la presente ley surge como respuesta a la necesidad imperante

de establecer un marco normativo que regule la Educación Digital y garantice la protección efectiva de los datos personales en todas las instancias, tanto públicas como privadas, en el territorio peruano

El acceso a la tecnología digital es ahora un elemento central en la vida de los ciudadanos, desde la educación hasta la participación en la esfera pública. La Educación Digital se revela como un instrumento crucial para empoderar a la sociedad en el uso ético, seguro y responsable de las herramientas digitales. Esta ley reconoce la necesidad de fomentar la alfabetización digital desde los primeros niveles educativos hasta la formación continua.

En este escenario, la protección de datos personales emerge como un pilar fundamental. El respeto a la privacidad se convierte en un imperativo ético y legal, garantizando que la recopilación, tratamiento y almacenamiento de datos personales se realicen de manera transparente, segura y respetuosa con los derechos individuales.

La propuesta de ley se fundamenta en la convicción de que la protección de datos y los derechos digitales son esenciales para preservar la dignidad, autonomía y libertad de los ciudadanos en el entorno digital. Estos derechos no son meramente una consecuencia de la evolución tecnológica, sino principios que deben ser resguardados activamente para mantener una sociedad justa e igualitaria.

El propósito de esta ley es establecer una política pública que garantice la adopción generalizada de prácticas seguras y éticas en el ámbito digital. Abarca tanto a las instituciones públicas como privadas, reconociendo que ambas tienen

responsabilidades cruciales en la salvaguarda de los derechos digitales y la protección de datos personales.

La urgencia de esta ley radica en la necesidad de anticiparse y prepararse para los desafíos venideros. La tecnología continuará evolucionando, y con ella, las amenazas potenciales a la privacidad y los derechos digitales. Establecer ahora una política clara y robusta es esencial para construir una sociedad digital justa, equitativa y segura.

La ley propuesta busca alinearse con estándares internacionales, reconociendo que la protección de datos y la educación digital son preocupaciones globales. Esto fortalecerá la posición de Perú en la comunidad internacional y facilitará la cooperación en la protección de datos transfronteriza.

Por ende la presente ley es un paso crucial hacia la construcción de un entorno digital que respete los derechos fundamentales de los ciudadanos. A través de la educación, la concientización y la regulación efectiva, aspira a forjar una sociedad digital inclusiva, ética y orientada al bienestar colectivo.

La Constitución Política del Perú de 1993 establece en su artículo 2, inciso 6, el derecho fundamental a la protección de datos personales. Este reconocimiento constitucional subraya la importancia de resguardar la privacidad y la información personal de los ciudadanos. Asimismo, en el artículo 2, inciso 5, se establece el derecho a la libertad de información, creando un equilibrio que esta ley busca articular de manera armoniosa.

La Ley de Protección de Datos Personales en el Perú (Ley N.º 29733) establece los principios y disposiciones para el tratamiento adecuado de los datos

personales. La presente ley de Educación Digital y Protección de Datos se erige como una extensión y complemento de la legislación existente, enfocándose específicamente en la dimensión educativa y su interrelación con la protección de datos personales.

El Perú, como signatario de diversas convenciones internacionales, reconoce la importancia de alinear su legislación con los estándares globales en materia de protección de datos y derechos digitales. Esta ley busca cumplir con los principios establecidos en tratados como el Convenio 108 del Consejo de Europa y contribuir a la armonización de normativas a nivel internacional.

El vertiginoso avance de la tecnología demanda un enfoque proactivo para empoderar a los ciudadanos con las habilidades necesarias para enfrentar los retos digitales. La educación digital se presenta como un componente esencial para fomentar un uso ético, seguro y responsable de la tecnología, y al mismo tiempo, como una herramienta para proteger los derechos digitales.

La ley propuesta reconoce que la protección de datos personales y la promoción de derechos digitales son interdependientes. Busca establecer mecanismos que no solo preserven la privacidad de los individuos, sino que también fomenten un entorno digital que respete los derechos fundamentales, como el derecho al olvido digital, el derecho a la identidad digital y el derecho a la educación digital.

La exposición de motivos reconoce los desafíos actuales, como la rápida evolución tecnológica, el aumento de ciberamenazas y la necesidad de preparar a la sociedad para un entorno digital en constante cambio. La ley busca ser adaptable y proactiva, proporcionando un marco que pueda evolucionar con las dinámicas tecnológicas y los nuevos desafíos que surjan.

En línea con los principios democráticos, la exposición de motivos destaca la necesidad de involucrar a la ciudadanía en el proceso de elaboración y revisión de políticas relacionadas con la protección de datos. La inclusión de la sociedad civil y la participación ciudadana contribuirá a leyes más equitativas y a la aceptación general de las medidas implementadas.

VIII.6. Propuesta de ley de educación digital y protección de datos

A continuación se presenta el proyectado de la ley que permita la implementación de la propuesta.

Capítulo I: Disposiciones Generales

Artículo 1: Definiciones

1. Educación Digital: Se refiere al conjunto de conocimientos, habilidades y actitudes necesarios para el uso ético, seguro y responsable de las tecnologías digitales.
2. Datos Personales: Toda información que identifica o hace identificable a una persona natural.
3. Autoridad de Educación Digital y Protección de Datos (AEDPD): Organismo creado para supervisar, regular y promover la educación digital y la protección de datos en instituciones públicas y privadas.

Artículo 2: Objetivos de la Ley

1. Promover la Educación Digital: Fomentar la integración de la Educación Digital en todos los niveles de la enseñanza formal y no formal en el país.
2. Proteger Datos Personales: Garantizar la protección efectiva de los datos personales en posesión de instituciones públicas y privadas.

3. Concientizar sobre Derechos Digitales: Impulsar la conciencia y respeto a los derechos digitales entre la población, destacando su importancia para la convivencia democrática.

Capítulo II: Implementación de la Educación Digital

Artículo 3: Integración Curricular

1. El Ministerio de Educación deberá incorporar la Educación Digital como parte integral del currículo educativo nacional en todos los niveles.
2. Se establecerán programas de formación continua para docentes, enfocados en las mejores prácticas de Educación Digital y protección de datos.

Artículo 4: Protección de Datos en Instituciones Públicas y Privadas

1. Se crea la Autoridad de Educación Digital y Protección de Datos (AEDPD) como ente regulador independiente.
2. La AEDPD supervisará y regulará el manejo de datos personales por parte de instituciones públicas y privadas.

Capítulo III: Supervisión y Regulación de Datos Personales

Artículo 5: Auditorías y Sanciones

1. La AEDPD llevará a cabo auditorías periódicas para evaluar el cumplimiento de las normativas de protección de datos.
2. Establecimiento de sanciones proporcionales a la gravedad de las infracciones cometidas.

Capítulo IV: Fomento a la Conciencia Digital

Artículo 6: Campañas de Concientización

1. Se implementarán campañas de concientización a nivel nacional sobre el uso ético y seguro de la tecnología y la importancia de la protección de datos.
2. Establecimiento de alianzas con organizaciones de la sociedad civil y empresas para promover prácticas seguras.

Capítulo V: Cooperación y Evaluación Continua

Artículo 7: Cooperación Internacional

1. La AEDPD colaborará con organismos internacionales para intercambiar experiencias y adoptar mejores prácticas en educación digital y protección de datos.

Artículo 8: Evaluación Periódica

1. Cada tres años se llevará a cabo una revisión integral de la ley para evaluar su efectividad y proponer ajustes según sea necesario.

Capítulo VI: Disposiciones Finales

Artículo 9: Vigencia

1. La ley entrará en vigencia seis meses después de su publicación oficial.
2. Los reglamentos para la implementación efectiva de la ley deberán ser emitidos por la AEDPD en un plazo máximo de tres meses de publicada la Ley.

VIII.7. Propuesta de Reglamento de Ley respecto a la educación digital y protección de datos

A continuación se presenta el Reglamento para la ley en mención y que permita la implementación de la propuesta.

Capítulo I: Disposiciones Generales

Artículo 1: Definiciones

1. Educación Digital: Se entenderá como el conjunto de conocimientos, habilidades y actitudes relacionadas con el uso ético, seguro y responsable de las tecnologías digitales.
2. Datos Personales: Cualquier información que identifica o hace identificable a una persona natural.

Capítulo II: Implementación de la Educación Digital

Artículo 2: Contenidos Curriculares

1. El Ministerio de Educación, en coordinación con la Autoridad de Educación Digital y Protección de Datos (AEDPD), establecerá los contenidos específicos de Educación Digital para cada nivel educativo.

Artículo 3: Formación Docente

1. El Ministerio de Educación implementará programas de formación continua para docentes, enfocados en las mejores prácticas de Educación Digital y protección de datos.

Capítulo III: Protección de Datos en Instituciones Públicas y Privadas

Artículo 4: Funciones de la AEDPD

1. La AEDPD tendrá las siguientes funciones:
 - a. Supervisar el manejo de datos personales por parte de instituciones públicas y privadas.
 - b. Evaluar y aprobar políticas internas de protección de datos.
 - c. Realizar auditorías y revisiones periódicas.

Artículo 5: Procedimientos de Auditoría

1. La AEDPD establecerá procedimientos y criterios para la realización de auditorías periódicas, considerando la magnitud y naturaleza de las operaciones de tratamiento de datos.

Artículo 6: Sanciones por Incumplimiento

1. Las sanciones por incumplimiento de las normativas de protección de datos serán proporcionales a la gravedad de las infracciones y podrán incluir multas, suspensiones temporales o cierres temporales de operaciones, según corresponda.

Capítulo IV: Fomento a la Conciencia Digital

Artículo 7: Campañas de Concientización

1. La AEDPD coordinará con el Ministerio de Transportes y Comunicaciones y la sociedad civil para diseñar y ejecutar campañas de concientización a nivel nacional.

Artículo 8: Colaboración con Empresas y Organizaciones

1. Se establecerán mecanismos de colaboración voluntaria con empresas y organizaciones para promover prácticas seguras y éticas en el manejo de datos.

Capítulo V: Cooperación y Evaluación Continua

Artículo 9: Cooperación Internacional

1. La AEDPD colaborará con organismos internacionales para compartir experiencias, buenas prácticas y fortalecer las capacidades en materia de educación digital y protección de datos.

Artículo 10: Evaluación Trienal

1. La AEDPD realizará una revisión completa de la implementación de la ley cada tres años, proponiendo ajustes o mejoras según sea necesario.

Capítulo VI: Disposiciones Finales

Artículo 11: Vigencia

1. El presente reglamento entra en vigencia al día siguiente de su publicación.

Artículo 12: Reglamentación Complementaria

1. La AEDPD emitirá reglamentos complementarios para la implementación efectiva de la ley en un plazo máximo de tres meses.

BIBLIOGRAFIA

- Akrivopoulou, C. M. (2012). *Human rights and risks in the digital era: Globalization and the effects of information technologies*. Idea Group.
<https://doi.org/10.4018/978-1-4666-0891-7>
- Alvear Richards, G. E., & Hernández Pesantes, E. A. (2023). *Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos*. <http://dspace.ups.edu.ec/handle/123456789/25257>
- Anstis, S., & Barnett, S. (2022a). Digital transnational repression and host states' obligation to protect against human rights abuses. *J. Hum. Rights Pract.*, 14(2), 698–725. <https://doi.org/10.1093/jhuman/huab051>
- Anstis, S., & Barnett, S. (2022b). Digital transnational repression and host states' obligation to protect against human rights abuses. *J. Hum. Rights Pract.*, 14(2), 698–725. <https://doi.org/10.1093/jhuman/huab051>
- Aponte, W. I. G. (2022). Derecho Fundamental a la protección de datos personales para las personas LGBTIQA+ en Brasil: Desafíos regulatorios para el futuro. *International Journal of Digital Law*.
<https://doi.org/10.47975/jdl.aponte.v.3.n.2>
- Awaghade, A. B. (2022). Online education - issues and challenges in digital equality matters. *Int. J. Hum. Rights Const. Stud.*, 9(4), 369.
<https://doi.org/10.1504/ijhracs.2022.126183>

Ballarín, L. B., Baigorri, L., Mengual, P. O., & Ortuño, P. (2021). ArchID (Archivo de Identidad Digital) iberoamericano Proyectos artísticos en torno al cuerpo, la autorrepresentación y la construcción identitaria. *Cuerpos Conectados. Arte, Identidad y Autorrepresentación En La Sociedad Transmedia*.
<https://doi.org/10.2307/j.ctv1s7cjm5.13>

Barrio, M. B. (2021). Génesis y desarrollo de los derechos digitales. *Revista de Las Cortes Generales*, 110, 197–233.
<https://doi.org/10.33426/RCG/2021/110/1572>

Baz Rodríguez, J. (2019). La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático. *Trabajo y Derecho: Nueva Revista de Actualidad y Relaciones Laborales*, ISSN 2386-8090, ISSN-e 2386-8112, Nº. 54, 2019, Págs. 49-78, 54, 49–78.
<https://dialnet.unirioja.es/servlet/articulo?codigo=6971659&info=resumen&idioma=SPA>

Bello, Z. O. (2021). EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN CUBA. DESAFÍOS EN LA ERA DIGITAL. *Revista IUS*.
<https://doi.org/10.35487/rius.v15i48.2021.689>

Benoit, M. B. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales. *Revista Chilena de Derecho y Tecnología*.
<https://doi.org/10.5354/0719-2584.2022.67205>

Berdote, E. B. (2022). La fragilidad del derecho fundamental a la protección de datos personales del menor ante la exposición de su vida personal y familiar

en la red: De la necesidad de nuevos mecanismos y garantías legales.

Estudios de Deusto. <https://doi.org/10.18543/ed.2646>

Berrocal-Lanzarot, A. (2020). *Estudio jurídico-crítico sobre la ley orgánica 3/2018*.

<https://books.google.es/books?hl=es&lr=&id=jpPSDwAAQBAJ&oi=fnd&pg=PA7&dq=estudios+de+proteccion+de+datos+personales+y+su+relacion+con+los+derechos+digitales&ots=EDU4FT4SoN&sig=UGXPrkKMqF3BTnxkMhloaYtRn04#v=onepage&q=estudios de proteccion de datos persona>

Bizberge, A., Segura, M. S., Bizberge, A., & Segura, M. S. (2020). Los derechos digitales durante la pandemia COVID-19 en Argentina, Brasil y México. *Revista de Comunicación*, 19(2), 61–85. <https://doi.org/10.26441/RC19.2-2020-A4>

Blanco, V. M. (2022). DERECHOS PERSONALÍSIMOS Y DATOS DIGITALES. In *Libertad para ordenar la sucesión. Libertad de testar* (pp. 406–411). Dykinson. <https://doi.org/10.2307/j.ctv2s0j7hz.35>

Bolívar Oñoro, M. D. V. (2020). Reseña a la obra de ARENAS RAMIRO, M.; ORTEGA GIMENEZ, A. (Directores): “Protección de Datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)”. Sepin, Madrid, 2019, 552 págs. *Rev. Derecho UNED (RDUNED)*, 26, 621. <https://doi.org/10.5944/rduned.26.2020.29207>

Bonet Navarro, J. (2021a). *HUMAN RIGHTS Evolution in the digital era*. Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie. <https://doi.org/10.13166/wsge/hr-pl/thaz5155>

- Bonet Navarro, J. (2021b). *HUMAN RIGHTS Evolution in the digital era*. Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie. <https://doi.org/10.13166/wsge/hr-pl/thaz5155>
- Carrillo, F. N. R. (2021a). *Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador*. <https://doi.org/10.18272/ulr.v8i1.2184>
- Carrillo, F. N. R. (2021b). *Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador*. <https://doi.org/10.18272/ulr.v8i1.2184>
- Castellanos Claramunt, J. (2020a). La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Métodos Inf.*, 11(21), 59–82. <https://doi.org/10.5557/iime11-n21-059082>
- Castellanos Claramunt, J. (2020b). La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Métodos Inf.*, 11(21), 59–82. <https://doi.org/10.5557/iime11-n21-059082>
- Chupillón Monsalve, A. L., & Vallejos Huamán, L. E. (2018). *Análisis doctrinal del llamado derecho al olvido dentro del ámbito jurídico tutelar peruano de protección de datos personales: derechos arco*. <https://tesis.usat.edu.pe/handle/20.500.12423/1551>

Díaz, A., & Página, G. (2023). *ANONIMIZACIÓN DE DATOS PERSONALES EN PROCESOS IMPLICADOS INFANTES Y ADOLESCENTES. LAS REGLAS DE HEREDIA.*

[https://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/C0C7BA87B5D40B81052577DD007B7C64/\\$FILE/diaz_8.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/C0C7BA87B5D40B81052577DD007B7C64/$FILE/diaz_8.pdf)

Díaz, M. F. S. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo.*
<https://doi.org/10.14409/redoeda.v10i1.12626>

Digital, R. L. G. de C. (2019). *Materiales de formación para estudiantes de grado de la Competencia Digital 4. Seguridad: 4.2. Protección de datos personales e identidad digital: 1. Definición de identidad digital y riesgos.*
<https://www.semanticscholar.org/paper/58abd064317acb72743730c9c959a45978f6fc05>

Duque, F. R. (2019). *La incidencia de la nueva Ley de Protección de Datos Personales y Garantía de los Derechos Digitales en los empleados públicos locales.*
<https://www.semanticscholar.org/paper/c78c961174ef52acb7c2f7f987e9cac341b6f12f>

Etxebarria, G. G. (2019). *Protección de datos personales y garantía de los derechos digitales. Ley Orgánica 3/2018, de 5 de diciembre.*
<https://www.semanticscholar.org/paper/5f7bc4f076d5418ebb5c7ba0df3e8c2c566b9bfd>

- Fernández, M. L. G. (2022). Los derechos digitales en la Ley Orgánica 3/2018, de Protección de Datos Personales y de garantía de los derechos digitales. *Asamblea. Revista Parlamentaria de La Asamblea de Madrid*. <https://doi.org/10.59991/rvam/2022/n.42/19>
- Font, I. G. (2019). *El interés jurídico protegido en el derecho a la seguridad digital: A propósito de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. <https://www.semanticscholar.org/paper/e1229e3d5cf802eb482d99bf4ec00474dc58f288>
- Ganesan, D. (2022). Human rights implications of the digital revolution in health care in India. *Health Hum. Rights*, 24(1), 5–19.
- Garcia, D. F., & Perea, A. Q. (2020). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Derecho PUCP*, 84, 271–299. <https://doi.org/10.18800/DERECHOPUCP.202001.009>
- Gázquez, A. E. (2022). Los derechos digitales:: Apertura del debate jurídico para su concreción y desarrollo. In *La Administración Digital* (pp. 141–170). Dykinson, S.L. <https://doi.org/10.2307/j.ctv2gz3vs4.9>
- González, Á. P. (2020a). *E-Justicia e Identidad Digital: un nuevo horizonte*.
- González, Á. P. (2020b). *E-Justicia e Identidad Digital: un nuevo horizonte*. <https://www.semanticscholar.org/paper/7511533431ac9b02690a66e3c45d3f554adeffe1>

González, E. G. (2017). *Big data, privacidad y protección de datos: Accésit 2015*.

https://books.google.es/books?hl=es&lr=&id=YteXEAAQBAJ&oi=fnd&pg=PA5&dq=estudios+de+proteccion+de+datos+personales+y+su+relacion+con+los+derechos+digitales&ots=8RC5xHFpzk&sig=s8U7GkKre4Efbko6KgMHeFPd_2Y#v=onepage&q&f=false

González-Patiño, J., & Esteban-Guitart, M. (2021). *La transformación hacia experiencias expandidas en educación superior: curso #UAMskills de identidad digital*. <https://doi.org/10.6018/red.433881>

HERAS HERNANDEZ, M. D. MAR. (2020). *Antecedentes y fundamentos del Derecho a la protección de datos*. 1–152.

Hernandez Palma, O. I. (2022). Pluralismo jurídico del siglo xxi y los derechos digitales: reflexiones en torno a la sentencia su-420 de 2019 de la Corte Constitucional Colombiana. *Justicia*, 27(41), 137–149. <https://doi.org/10.17081/just.27.41.5702>

Huerta, G., & Cochachin, M. (2021a). *Derecho al olvido digital como solución al conflicto entre la libertad de información y el derecho de protección de datos personales en el Perú*.

Huerta, G., & Cochachin, M. (2021b). *Derecho al olvido digital como solución al conflicto entre la libertad de información y el derecho de protección de datos personales en el Perú*. <https://repositorio.unasam.edu.pe/handle/UNASAM/4812>

- Ibarra, G. E. (2023). La inviolabilidad de las comunicaciones desde la protección de datos personales. *Estudios Políticos*.
<https://doi.org/10.22201/fcpys.24484903e.2023.60.86872>
- Jiménez, L. M., & García-Ferrería, J. P. (2015). Sobre el derecho al olvido digital:: una solución al conflicto entre la libertad de información y el derecho de protección de datos personales en los motores de búsqueda. *Rev. RJUAM*, 32. <https://revistas.uam.es/revistajuridica/article/view/6443>
- Kirchschlaeger, P. G. (2019). Digital transformation of society and economy - ethical considerations from a human rights perspective. *Int. J. Hum. Rights Const. Stud.*, 6(4), 301. <https://doi.org/10.1504/ijhracs.2019.10024214>
- León, J. Á. Q., León, Q., & Álvaro, J. (2021). Ciberseguridad y protección de datos personales en el Perú. *ADVOCATUS*.
<https://doi.org/10.26439/advocatus2021.n39.5114>
- Lombarte, A. (2020a). Una nueva generación de derechos digitales. *Revista de Estudios Políticos*, ISSN 0048-7694, N° 187, 2020, Págs. 101-135, 187(187), 101–135. <https://doi.org/10.18042/cepc/rep.187.04>
- Lombarte, A. (2020b). Una nueva generación de derechos digitales. *Revista de Estudios Políticos*, ISSN 0048-7694, N° 187, 2020, Págs. 101-135, 187(187), 101–135. <https://doi.org/10.18042/cepc/rep.187.04>
- Lugo, M. T., & Ithurburu, V. (2020). Las políticas digitales en educación: Una cuestión de derechos. In *Tecnologías digitales y transformaciones sociales*

(pp. 97–112). Consejo Latinoamericano de Ciencias Sociales. CLACSO.
<https://doi.org/10.2307/j.ctv1gm00zt.8>

Luna Cervantes, E. J. (2021a). Preguntas y respuestas varias sobre la protección de datos personales en el Perú. *Advocatus*, 039, 253–264.
<https://doi.org/10.26439/advocatus2021.n39.5133>

Luna Cervantes, E. J. (2021b). Preguntas y respuestas varias sobre la protección de datos personales en el Perú. *Advocatus*, 039, 253–264.
<https://doi.org/10.26439/advocatus2021.n39.5133>

Maréchal, N., & Project, R. D. R. (2015). FCJMESH-009 ranking digital rights: Keeping the internet safe for advocacy. *Fibreculture J.*, 26, 302–308.
<https://doi.org/10.15307/fcj.mesh.009.2015>

Milan, S., & Velden, L. van der. (2016). The Alternative Epistemologies of Data Activism. *Digital Culture & Society*, 2(2), 57–74.
<https://doi.org/10.14361/DCS-2016-0205>

Minero, G. (2014). A vueltas con el derecho al olvido : construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital. *Revista Jurídica : Universidad Autónoma de Madrid : 30, II, 2014*, 129–155.

Morales, E., & Lidette, A. (2022). *Las llamadas comerciales efectuadas por entidades financieras y la vulneración del derecho constitucional a la protección de datos personales*.
<https://repositorio.ucv.edu.pe/handle/20.500.12692/114312>

- Moreno Bobadilla, Á. (2020a). Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital. *Estud. Const. (Impresa)*, 18(2), 121–150. <https://doi.org/10.4067/s0718-52002020000200121>
- Moreno Bobadilla, Á. (2020b). Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital. *Estud. Const. (Impresa)*, 18(2), 121–150. <https://doi.org/10.4067/s0718-52002020000200121>
- Muñoz, F. S. (2021). El derecho a la protección de datos personales frente al uso de las TIC. *Revista Internacional de Ciencias Sociales Interdisciplinarias*. <https://doi.org/10.18848/2474-6029/cgp/v10i01/23-34>
- Olivares, R. S. (2019). Los Derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. *IusLabor*. <https://doi.org/10.31009/iuslabor.2018.i03.06>
- Patraca, G. A. H., Kiss, G., Gastelú, C. A. T., & Domínguez, A. L. (2021). *Diseño y validación de una escala para medir la gestión de la identidad digital*. <https://doi.org/10.23913/ride.v11i22.943>
- Pilege, E., Plota, S., Pilegis, G., Zivitere, M., Luchev, D., & Goynov, M. (2022). The role of the digital environment in the context of cultural rights. *DiPP*, 12, 111–120. <https://doi.org/10.55630/dipp.2022.12.8>

- Pineda, L. O., Quezada, L. C., Quezada, L. C., & Conde, A. C. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado y Comunes*. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270
- Polo-Roca, A. (2020a). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Rev. Derecho Político*, 108, 165–194. <https://doi.org/10.5944/rdp.108.2020.27998>
- Polo-Roca, A. (2020b). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Rev. Derecho Político*, 108, 165–194. <https://doi.org/10.5944/rdp.108.2020.27998>
- Porcelli, A. M. (2019). *Vista do La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos*. <https://doi.org/10.12957/rqi.2019.40175>
- Rallo Lombarte, A. (2020). Una nueva generación de derechos digitales. *Rev. Estud. Políticos*, 187, 101–135. <https://doi.org/10.18042/cepc/rep.187.04>
- Ramírez, M. F. D., & Vázquez, A. F. Z. (2023). Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. *MQRInvestigar*. <https://doi.org/10.56048/mqr20225.7.1.2023.330-343>
- Ramiro, M. A. (2021). NUEVAS TECNOLOGÍAS Y RETOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA: El rastreo de contactos durante la pandemia por covid-19. *Confluências | Revista*

<https://doi.org/10.22409/conflu.v23i2.50519>

Rank, A. T., & Berberi, M. A. L. (2022). Big data e direitos fundamentais sob o enfoque da Lei Geral de Proteção de Dados (LGPD): Big data and fundamental rights under the approach of the General Data Protection Law (GDPL). *Intl. J. Digital Law*, 3(2), 9–26. <https://doi.org/10.47975/ijdl.rank.v.3.n.2>

Revoredo-Palacios, A. (2021). Publicidad programática y protección de datos personales. *Advocatus*, 039, 149–157. <https://doi.org/10.26439/advocatus2021.n39.5124>

Rights, U. N. O. of the H. C. on H. (2022). *Berkeley Protocol on digital open source investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law*. United Nations.

Roca, A. P. (2020a). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, 108, 165–194. <https://doi.org/10.5944/RDP.108.2020.27998>

Roca, A. P. (2020b). *El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado*. <https://doi.org/10.5944/rdp.108.2020.27998>

Rochel, J. (2021). Connecting the dots: Digital integrity as a human right. *Hum. Rights Law Rev.*, 21(2), 358–383. <https://doi.org/10.1093/hrlr/ngaa063>

- Rodríguez, R. V. (2022). La responsabilidad proactiva en la normativa peruana de protección de datos personales. *Yachaq*.
<https://doi.org/10.51343/yq.vi13.913>
- Rúa, M. M. B., & Tapiero, J. I. M. (2021). Justicia digital, acceso a internet y protección de datos personales. *Revista Internacional de Derecho*.
<https://doi.org/10.37768/unw.rid.02.01.001>
- Rudas Chara, C. A., & Carpio Romero, C. K. (2022). *Afectación al derecho a la privacidad por la indebida protección de datos personales de los usuarios en el Banco de Crédito, 2021*.
- Saavedra-Grados, C. (2023). *Uso de datos personales, y el derecho a la protección a la intimidad de las personas en Tarapoto 2020-2022*.
- Salinas, A., & Vasquez, J. (2023a). *Nivel de cumplimiento de la ley de protección de datos personales en la gestión de los bancos de datos de historias clínicas del Centro Médico San Pablo en el año 2021*.
- Salinas, A., & Vasquez, J. (2023b). *Nivel de cumplimiento de la ley de protección de datos personales en la gestión de los bancos de datos de historias clínicas del Centro Médico San Pablo en el año 2021*.
<https://repositorio.upn.edu.pe/handle/11537/33495>
- Samper, M. B. (2020). LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES. In *Protección de datos personales* (pp. 145–252). Dykinson. <https://doi.org/10.2307/j.ctv17hm980.5>

Segura, M. S. (2019). Activismo por los derechos digitales en América Latina.

Pensar globalmente, actuar localmente. *Segura, Maria Soledad; Activismo Por Los Derechos Digitales En América Latina. Pensar Globalmente, Actuar Localmente; Universidad Alberto Hurtado; Persona y Sociedad, 33, 2; 12.*

Serna, F. J. A. (2021a). DELIMITACIÓN DEL DERECHO A LA INTIMIDAD EN INTERNET. In *Derecho y nuevas tecnologías. La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español* (pp. 113–122). Dykinson. <https://doi.org/10.2307/j.ctv2gz3tdz.13>

Serna, F. J. A. (2021b). HACIA UNA MEJOR REGULACIÓN JURÍDICA DE INTERNET:: LA NECESIDAD DE UN ORDENAMIENTO JURÍDICO VIRTUAL. In *Derecho y nuevas tecnologías. La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español* (pp. 165–168). Dykinson. <https://doi.org/10.2307/j.ctv2gz3tdz.21>

Serna, F. J. A. (2021c). LA RELACIÓN ENTRE DERECHO Y TECNOLOGÍA. In *Derecho y nuevas tecnologías. La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español* (pp. 23–36). Dykinson. <https://doi.org/10.2307/j.ctv2gz3tdz.6>

Serna, F. J. A. (2021d). MECANISMOS DE REGULACIÓN DE LA TECNOLOGÍA. In *Derecho y nuevas tecnologías. La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento*

jurídico español (pp. 51–66). Dykinson.
<https://doi.org/10.2307/j.ctv2gz3tdz.8>

Serna, F. J. A. (2021e). NECESIDAD DE LA REGULACIÓN TECNOLÓGICA. In *Derecho y nuevas tecnologías. La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español* (pp. 37–50). Dykinson.
<https://doi.org/10.2307/j.ctv2gz3tdz.7>

Siagian, R., Siahaan, L., & Hamzah, M. I. (2023). Human rights in the digital era: Online privacy, freedom of speech, and personal data protection. *J. Dig. Learning and Dist. Edu*, 2(4), 513–523.
<https://doi.org/10.56778/jdlde.v2i4.149>

Susi, M. (2021). *Human rights, digital society and the law: A research companion*. Routledge.

Vázquez-Cano, E., & Pascual -Moscoso, C. (2022a). Protección de datos y uso ético de la tecnología para una didáctica sostenible. *Rev. Electrón. Interuniv. Form. Profr.*, 25(3), 95–110. <https://doi.org/10.6018/reifop.529831>

Vázquez-Cano, E., & Pascual -Moscoso, C. (2022b). Protección de datos y uso ético de la tecnología para una didáctica sostenible. *Rev. Electrón. Interuniv. Form. Profr.*, 25(3), 95–110. <https://doi.org/10.6018/reifop.529831>

Wagner, B., Kettemann, M. C., & Vieth, K. (2020). *Research handbook on human rights and digital technology: Global politics, law and international relations*. Edward Elgar Publishing.

Wu, T. (2005). Network Neutrality, Broadband Discrimination. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.388863>

Ziccardi, G. (2014). *Resistance, liberation technology and human rights in the digital age* (2013th ed.). Springer.

ANEXOS

Anexo 1: Matriz de consistencia

PROBLEMA	HIPOTESIS	OBJETIVO	VARIABLE
Problema General ¿Cómo la protección de datos personales se relaciona con los derechos digitales en el Perú?	Hipótesis General Existe relación entre la protección de datos personales y los derechos digitales en el Perú	Objetivo General Determinar cómo la protección de datos personales se relaciona con los derechos digitales en el Perú	Variable 01: Protección de datos personales • <u>Dimensión 1:</u> Seguridad y protección • <u>Dimensión 2:</u> Finalidad legítima y limitada • <u>Dimensión 3:</u> Consentimiento informado
Problemas Específicos Problema Especifico 1 ¿Cómo la protección de datos personales se relaciona con la privacidad y confidencialidad digital en el Perú?	Hipótesis específicas Hipótesis específica 01 Existe relación entre la protección de datos personales y la privacidad y confidencialidad digital en el Perú	Objetivo Especificas Objetivo Especifico 1 Determinar cómo la protección de datos personales se relaciona con la privacidad y confidencialidad digital en el Perú	
Problema Especifico 2 ¿Cómo la protección de datos personales se relaciona con el derecho al olvido digital en el Perú?	Hipótesis específica 02 Existe relación entre la protección de datos personales y el derecho al olvido digital en el Perú.	Objetivo Especifico 2 Determinar cómo la protección de datos personales se relaciona con el derecho al olvido digital en el Perú	
			Variable 02: Derechos digitales • <u>Dimensión 1:</u> Privacidad y confidencialidad

Problema Especifico 3 ¿Cómo la protección de datos personales se relaciona con el derecho a la identidad digital en el Perú?	Hipótesis específica 03 Existe relación entre la protección de datos personales y derecho a la identidad digital en el Perú.	Objetivo Especifico 3 Determinar cómo la protección de datos personales se relaciona con el derecho a la identidad digital en el Perú	• <u>Dimensión 2:</u> Derecho al olvido • <u>Dimensión 3:</u> Derecho a la identidad digital • <u>Dimensión 4:</u> Derecho a la educación digital
Problema Especifico 4 ¿Cómo la protección de datos personales se relaciona con el derecho a la educación digital en el Perú?	Hipótesis específica 04 Existe relación entre la protección de datos personales y derecho a la educación digital en el Perú.	Objetivo Especifico 4 Determinar cómo la protección de datos personales se relaciona con el derecho a la educación digital en el Perú	

Anexo 2: Matriz de Operacionalización variable Protección de datos personales

Matriz de Operacionalización de la variable Protección de datos personales				
Dimensiones	Indicadores	Ítems	Escala	Niveles
Dimensión 1: Seguridad y protección	- Existencia de medidas de seguridad tecnológicas, como cifrado de datos, cortafuegos y antivirus, implementadas para proteger la información personal. - Capacitación regular del personal en prácticas de seguridad de datos y conciencia de las amenazas cibernéticas. - Registro y seguimiento de incidentes de seguridad de datos, como brechas o intentos de acceso no autorizado. - Evaluación periódica de vulnerabilidades y auditorías de seguridad para garantizar la protección de datos. - Cumplimiento de estándares de seguridad reconocidos, como ISO 27001 o normativas específicas del sector.	01-04	Ordinal 1 = Totalmente en desacuerdo 2 = En desacuerdo 3 = Neutral 4 = De acuerdo 5 = Totalmente de acuerdo	Bajo=12-24 Medio=25-48 Alto= 49-60
Dimensión 2:	- Documentación clara de los propósitos para los cuales se recopilan datos personales. - Revisión periódica de la idoneidad de los fines para los cuales se utilizan los datos personales.	05-08		

Finalidad legítima y limitada	• Implementación de políticas que prohíban el uso de datos personales para fines distintos de los declarados sin el consentimiento explícito del titular. • Procedimientos de revisión de la finalidad del procesamiento de datos en caso de cambios en las circunstancias. • Verificación de que los datos personales no se almacenan durante más tiempo del necesario para los fines declarados.			
Dimensión 3: Consentimiento informado	• Obtención de consentimiento claro y específico de los titulares de datos antes de recopilar o procesar sus datos personales. • Documentación de los procedimientos utilizados para obtener y registrar el consentimiento. • Garantía de que los titulares de datos estén debidamente informados sobre cómo se utilizarán sus datos personales. • Provisión de mecanismos para que los titulares de datos retiren su consentimiento en cualquier momento. • Verificación de que el consentimiento se renueve si se cambian los fines de procesamiento de datos.	09-12		

Anexo 3: Matriz de Operacionalización variable Derechos Digitales

Matriz de Operacionalización de la variable Derechos digitales				
Dimensiones	Indicadores	Ítems	Escala	Niveles
Dimensión 1: Privacidad y confidencialidad	• Proporción de usuarios que ajustan sus configuraciones de privacidad en redes sociales y servicios en línea. • Número de denuncias de violaciones de privacidad en línea. • Grado de conciencia pública sobre las prácticas de recolección y uso de datos por parte de las empresas. • Implementación de regulaciones de protección de datos y sus efectos en la protección de la privacidad en línea.	01-04	Ordinal 1=Totalmente en desacuerdo 2=En desacuerdo 3=Neutral	Bajo=16-32 Medio=33-64 Alto= 65-80
Dimensión 2: Derecho al olvido	• Número de solicitudes de eliminación de información personal en motores de búsqueda. • Tasa de cumplimiento de las solicitudes de derecho al olvido. • Evaluación de la efectividad de la eliminación de información en la restauración de la privacidad y la reputación en línea.	05-08	4=De acuerdo 5=Totalmente de acuerdo	

	• Casos de controversia relacionados con el derecho al olvido y su resolución.			
Dimensión 3: Derecho a la identidad digital	• Nivel de autenticación y verificación en línea requerido para acceder a servicios digitales. • Número de casos de robo de identidad digital. • Medidas de seguridad implementadas en la gestión de identidades digitales, como la autenticación de dos factores. • Tasa de adopción de sistemas de gestión de identidades digitales descentralizadas.	09-12		
Dimensión 4: Derecho a la educación digital	• Acceso a la educación digital, incluido el acceso a Internet y dispositivos para la educación en línea. • Inversión en programas de alfabetización digital y educación en línea. • Evaluación de la calidad y la disponibilidad de contenido educativo en línea. • Participación y finalización de cursos y programas de educación digital.	12-16		

Anexo 4: Declaración de Originalidad del Asesor

DECLARATORIA DE AUTENTICIDAD DEL ASESOR

Yo, Dr. CUETO CHUMÁN, PEDRO GUSTAVO ALBERTO docente de la Facultad de Derecho y Ciencias Políticas, adscrito a la Escuela de Derecho de la Universidad Nacional Mayor de San Marcos, asesor de la tesis titulada: “La protección de datos personales y su relación con los derechos digitales en la legislación peruana”, del autor Aguilar Hernando, Jorge Vladimir, constato que la investigación tiene un índice de similitud de 20% verificable en el reporte de originalidad del programa Turnitin adjunto a la presente.

He revisado dicho reporte y concluye que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender al proyecto de investigación cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Mayor de San Marcos.

Lima, 12 de noviembre 2023

Dr. CUETO CHUMÁN, PEDRO GUSTAVO ALBERTO	
DNI: 10474687	Firma



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Universidad del Perú. Decana de América

Facultad de Derecho y Ciencias Políticas

Escuela Profesional de Derecho

La protección de datos personales y su relación
con los derechos digitales en la legislación peruana

Tesis

Para optar el Título Profesional de Abogado

Autor

Aguilar Hernando, Jorge Vladimir

Asesor

Dr. Cuello Shumian, Pedro Gustavo Alberto

2023



Resumen de coincidencias

20 %

< >

Se están viendo fuentes estándar

EN Ver fuentes en inglés

Coincidencias

1	hdl.handle.net	3 %	>
	Fuente de Internet		
2	www.informatica-juridi...	3 %	>
	Fuente de Internet		
3	Entregado a Universida...	1 %	>
	Trabajo del estudiante		
4	Entregado a Universida...	1 %	>
	Trabajo del estudiante		
5	ijj.ucr.ac.cr	1 %	>
	Fuente de Internet		
6	Entregado a Universida...	1 %	>
	Trabajo del estudiante		
7	Entregado a Universida...	1 %	>
	Trabajo del estudiante		
8	ifai.org.mx	1 %	>
	Fuente de Internet		
9	repositorio.una.edu.pe	1 %	>
	Fuente de Internet		

Anexo 5: Declaración de Originalidad del Autor

DECLARATORIA DE ORIGINALIDAD DEL AUTOR

Yo, Jorge Vladimir Aguilar Hernando, egresado de la Escuela de Derecho de la Universidad Nacional Mayor de San Marcos, declaro bajo juramento que todos los datos e información que acompañan a la tesis titulada: “La protección de datos personales y su relación con los derechos digitales en la legislación peruana”, es de mi autoría, por lo tanto, declaro que la tesis:

- No ha sido plagiado ni total, ni parcialmente.
- He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
- No ha sido publicado ni presentado anteriormente para la obtención de otro grado académico o título profesional.
- Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad

Lima, 12 de noviembre 2023

Aguilar Hernando, Jorge Vladimir	
DNI: 07973691	
ORCID (orcid.org/ 0000-0002-4652-2774)	

Anexo 6: Formato de Encuesta

Cuestionario sobre la Protección de Datos Personales

Instrucciones: Para cada afirmación, indica en qué medida estás de acuerdo o en desacuerdo con ella, utilizando la escala de 1 a 5, donde:

1 = Totalmente en desacuerdo

2 = En desacuerdo

3 = Neutral

4 = De acuerdo

5 = Totalmente de acuerdo

	1 = Totalmente en desacuerdo	2 = En desacuerdo	3 = Neutral	4 = De acuerdo	5 = Totalmente de acuerdo
Dimensión 1: Seguridad y protección					
1. Los servicios y plataformas digitales en los que interactúo protegen adecuadamente mis datos personales.					
2. Me siento seguro/a de que mis datos personales no serán accesibles para personas no autorizadas.					
3. Creo que las medidas de seguridad implementadas por las empresas y organizaciones son efectivas para proteger mi información personal.					
4. Considero que las instituciones gubernamentales tienen protocolos adecuados para proteger los datos personales de los ciudadanos.					
Dimensión 2: Finalidad legítima y limitada					
5. Las empresas y organizaciones utilizan mis datos personales únicamente con fines específicos y claros.					
6. Considero que las instituciones gubernamentales recolectan y utilizan los datos personales de manera responsable y con propósitos legítimos.					
7. Las empresas y organizaciones explican claramente cómo utilizarán mis datos personales antes de recopilarlos.					

8. Existe una regulación adecuada que limita la recolección y uso excesivo de datos personales en el país.					
Dimensión 3: Consentimiento informado					
9. Siempre me solicitan mi consentimiento antes de recolectar y utilizar mis datos personales.					
10. Me siento informado/a sobre cómo se utilizarán mis datos personales cuando proporciono mi consentimiento.					
11. Considero que las empresas y organizaciones respetan mi decisión si decido no dar mi consentimiento para el uso de mis datos personales.					
12. Creo que la información sobre el consentimiento se presenta de manera clara y comprensible.					

Cláusula de Confidencialidad y Protección de Datos

1. Confidencialidad de la Información:

El participante de esta encuesta reconoce que toda la información proporcionada es estrictamente confidencial. Los datos recopilados serán utilizados únicamente con fines estadísticos y de análisis, asegurando que la identidad de los participantes no sea divulgada en ninguna publicación o informe resultante.

2. Protección de Datos Personales:

De acuerdo con la Ley N° 29733, Ley de Protección de Datos Personales, se informa que los datos personales recolectados serán almacenados en una base de datos bajo responsabilidad del investigador. La información será tratada de manera adecuada y segura, garantizando la confidencialidad y el respeto a los derechos de los participantes.

3. Derechos de los Participantes:

Los participantes tienen derecho a acceder, rectificar y cancelar sus datos personales, así como a oponerse a su tratamiento. Para ejercer estos derechos, se deberá enviar una solicitud a [indicar el correo electrónico o dirección física de contacto].

4. Aceptación:

Al participar en esta encuesta, el participante acepta la presente cláusula de confidencialidad y protección de datos, confirmando que ha sido informado sobre el uso que se dará a su información.

Cuestionario sobre Derechos Digitales

Instrucciones: Para cada afirmación, indica en qué medida estás de acuerdo o en desacuerdo con ella, utilizando la escala de 1 a 5, donde:

1 = Totalmente en desacuerdo

2 = En desacuerdo

3 = Neutral

4 = De acuerdo

5 = Totalmente de acuerdo

	1 = Totalmente en desacuerdo	2 = En desacuerdo	3 = Neutral	4 = De acuerdo	5 = Totalmente de acuerdo
Dimensión 1: Privacidad y confidencialidad					
1. Considero que tengo control sobre la información personal que comparto en línea.					
2. Me siento seguro/a de que mis datos personales son tratados de forma confidencial en el entorno digital.					
3. Creo que mis comunicaciones electrónicas están protegidas y no son accesibles por terceros sin mi consentimiento.					
4. Siento que mis derechos de privacidad son respetados por las empresas y plataformas digitales que utilizo.					
Dimensión 2: Derecho al olvido					
5. Considero que tengo el derecho de solicitar la eliminación de información personal que ya no es relevante o precisa en el entorno digital.					
6. Siento que las empresas y plataformas digitales respetan mi derecho al olvido y eliminan mis datos personales cuando lo solicito.					
7. Me siento informado/a sobre cómo ejercer mi derecho al olvido en línea.					

8. Creo que las instituciones gubernamentales deben garantizar el derecho al olvido en el entorno digital.					
Dimensión 3: Derecho a la identidad digital					
9. Siento que mi identidad digital está protegida y no es fácilmente manipulable por otros.					
10. Considero que tengo control sobre cómo se utiliza mi identidad digital en diferentes plataformas y servicios en línea.					
11. Creo que las empresas y plataformas digitales respetan mi identidad digital y evitan que terceros la utilicen sin mi consentimiento.					
12. Me siento informado/a sobre cómo proteger mi identidad digital y mantenerla segura en el entorno digital.					
Dimensión 4: Derecho a la educación digital					
13. Existe una conciencia y comprensión adecuadas sobre la importancia de la educación digital en la sociedad.					
14. Las instituciones educativas y organizaciones promueven la educación digital y los derechos digitales entre los ciudadanos.					
15. Considero que tengo acceso a recursos y herramientas para aprender sobre educación digital y protección de derechos en el entorno digital.					
16. Me siento informado/a sobre mis derechos digitales y cómo ejercerlos en línea.					
Dimensión General de Derechos Digitales					

17. En general, considero que mis derechos digitales están bien protegidos en el entorno en línea.					
18. Siento que tengo el control sobre cómo se respetan mis derechos digitales en diferentes plataformas y servicios.					
19. Creo que existe una conciencia adecuada sobre la importancia de los derechos digitales en la sociedad.					
20. En general, considero que las instituciones gubernamentales y empresas respetan los derechos digitales de los ciudadanos.					

Cláusula de Confidencialidad y Protección de Datos

1. Confidencialidad de la Información:

El participante de esta encuesta reconoce que toda la información proporcionada es estrictamente confidencial. Los datos recopilados serán utilizados únicamente con fines estadísticos y de análisis, asegurando que la identidad de los participantes no sea divulgada en ninguna publicación o informe resultante.

2. Protección de Datos Personales:

De acuerdo con la Ley N° 29733, Ley de Protección de Datos Personales, se informa que los datos personales recolectados serán almacenados en una base de datos bajo responsabilidad del investigador. La información será tratada de manera adecuada y segura, garantizando la confidencialidad y el respeto a los derechos de los participantes.

3. Derechos de los Participantes:

Los participantes tienen derecho a acceder, rectificar y cancelar sus datos personales, así como a oponerse a su tratamiento. Para ejercer estos derechos, se deberá enviar una solicitud a [indicar el correo electrónico o dirección física de contacto].

4. Aceptación:

Al participar en esta encuesta, el participante acepta la presente cláusula de confidencialidad y protección de datos, confirmando que ha sido informado sobre el uso que se dará a su información.

