UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE DERECHO

ESCUELA DE DERECHO

Incorporación de la privacidad desde el diseño como principio fundamental que garantice el legítimo tratamiento de datos personales en Perú

TESIS PARA OPTAR EL TÍTULO DE ABOGADO

AUTOR

Palestina Sabina Vargas Toscanelli

ASESOR

Katherinee del Pilar Alvarado Tapia

https://orcid.org/0000-0002-8451-0475

Chiclayo, 2025

Incorporación de la privacidad desde el diseño como principio fundamental que garantice el legítimo tratamiento de datos personales en Perú

PRESENTADA POR

Palestina Sabina Vargas Toscanelli

A la Facultad de Derecho de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el título de

ABOGADO

APROBADA POR

Freddy Widmar Hernandez Rengifo
PRESIDENTE

Dora María Ojeda Arriarán
SECRETARIO

Katherinee del Pilar Alvarado Tapia
VOCAL

Dedicatoria

A Dios, por guiarme en cada paso que he dado, cada desafío que he enfrentado en este viaje académico, han sido posibles gracias a su sabiduría y amor

Agradecimiento

A mi familia, les debo una deuda de gratitud que no puede ser expresada completamente en palabras. Su amor inquebrantable y su apoyo constante me han sostenido en los momentos de desafío y me han brindado la motivación para seguir adelante.

Incorporación de la privacidad desde el diseño como principio fundamental que garantice el legítimo tratamiento de datos personales en Perú

INFORME DE ORIGINALIDAD

21%	23%	15%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	4%
2	www.tc.gob.pe Fuente de Internet	2%
3	tesis.usat.edu.pe Fuente de Internet	2%
4	www.udg.edu Fuente de Internet	1%
5	digibug.ugr.es Fuente de Internet	1%
6	e-revistas.uc3m.es Fuente de Internet	1%
7	tesis.pucp.edu.pe Fuente de Internet	1%
8	www.informatica-juridica.com Fuente de Internet	1%
9	habeasdatacolombia.uniandes.edu.co Fuente de Internet	1%
10	1library.co Fuente de Internet	<1%
11	pdffox.com Fuente de Internet	<1%

repositorio.unsa.edu.pe

Índice

Resumen

La presente investigación aborda como objetivo principal garantizar el legítimo tratamiento de datos personales mediante la incorporación del principio de la privacidad desde el diseño en la normativa peruana. A partir de esto, se determinaron tres objetivos específicos, los cuales son: (1) Analizar la relevancia constitucional de la tutela de derecho fundamental de protección de datos personales y evaluar su impacto en el tratamiento de datos, a partir de la doctrina y jurisprudencia comparada, (2) Determinar las consecuencias jurídicas de la aplicación del principio de privacidad desde el diseño a innovaciones tecnológicas; y , (3) Sustentar criterios que permitan materializar la privacidad desde el diseño como principio jurídico en el ordenamiento peruano. Seguidamente, como metodología se aplicó el método analítico y documental, al tratarse de una investigación cualitativa. Finalmente, se propone mediante criterios jurídicos, materializar la privacidad desde el diseño como principio en la normativa peruana, garantizando el legítimo tratamiento de datos personales.

Palabras clave: Privacidad desde el diseño, protección de datos personales, innovaciones tecnológicas y tratamiento de datos.

Abstract

This investigation has as a main objective to ensure the legitimate processing of personal data by incorporating the privacy by design principle into the peruvian regulations. As a consequence, three specific objectives were determined: (1) Analyze the constitutional relevance of the protection of the fundamental right to personal data and evaluate its impact on data processing based on doctrine and comparative jurisprudence, (2) Determine the legal consequences of applying the privacy by design principle to technological innovations, and (3) Provide criteria to materialize privacy by design as a legal principle in the Peruvian legal system. Subsequently, an analytical and documentary method was applied as it is qualitative research. Finally, through legal criteria, it is proposed to materialize privacy by design as a principle in Peruvian regulations, ensuring the legitimate processing of personal data.

Keywords: Privacy by design, personal data protection, technology innovations, and data treatment

1. Introducción

La privacidad desde el diseño es un concepto relativamente nuevo, que surge a raíz de resguardar la privacidad durante el ciclo de vida de las innovaciones tecnológicas y promete prevenir futuras brechas de seguridad, al basar su constitución en los principios de Practicas Justas de información creadas por el Departamento de Seguridad de Estados Unidos y posteriormente se desarrolló dentro del marco Europeo, regulándolo en su Reglamento 2016/ 679 del parlamento europeo, con la finalidad de "adelantarse a los hechos que puedan impactar la privacidad antes de que ocurran (…) y constituyendo un componente esencial e inseparable de los sistemas, programas, bienes y servicios, así como de las políticas empresariales y procedimientos internos de la entidad"

Es así que, el presente artículo aborda como la incorporación del principio de la Privacidad desde el Diseño en el Perú, representará un paso crucial hacia la protección efectiva del tratamiento de datos personales en un entorno digital en constante evolución, poniéndole énfasis en la consideración proactiva de la privacidad en todas las etapas de proyectos, sistemas y servicios que involucran datos personales, el cual, es posible aplicar conforme lo señala Majed Alshammari (2019), autor de la tesis doctoral: "A Principled Approach for Engineering Privacy by Design", quien destaca el protagonismo de la privacidad en las innovaciones tecnológicas y desarrolla un enfoque en materializar la privacidad desde el diseño a través de la ingeniería de privacidad.

El Foro Económico Mundial (2020) en el "Reporte de Riesgos Mundiales", determinó el incremento significativo de ataques cibernéticos en un 75%, específicamente de robo datos personales a nivel mundial y como en el 2021 los delitos por ciber crimen podrían alcanzar los 6 billones de dólares, equivalente al PBI de la tercera economía más grande del mundo. En consecuencia, las brechas informáticas siempre continuarán sucediendo, puesto que los softwares continuamente serán actualizados para incurrir en ataques cibernéticos.

Por tanto, cuando mencionamos ataques cibernéticos no solo hacemos referencia a filtración de datos o brechas de información, sino que también involucra la repercusión en la sociedad, pues el problema incurre en "para que" utilizan la información robada o sin consentimiento, ya que, actualmente existen muchos delitos informáticos, tales como, el robo de identidad, extorción, robo de cuentas bancarias, entre otros. Afectando la vida de las personas y la sociedad, porque involucra tanto como conozcan o no sobre tratamiento de datos, es así que el Estado está en la obligación de presentar garantías de seguridad.

También analizamos mediante la casuística, resoluciones de los procedimientos sancionadores y, como la Resolución Directoral N° 396-2023-JUS/DGTAIPD-DPDP de fecha

27 de febrero de 2023, resolvió sancionar a la entidad financiera BBVA por vulnerar el tratamiento de datos personales del denunciante con propósitos comerciales y de promoción, sin haber recabado de manera válida la autorización del titular de dichos datos.

Finalmente, hallamos que en el territorio nacional la Ley N° 29733 encargada de regular la Protección de Datos Personales y su reglamento, está constituida para ser por defecto y actúa cuando ya se lesiono los datos personales, sin embargo, es cierto que presenta ciertas limitaciones, particularmente en lo que respecta a la falta de un enfoque preventivo más sólido, pero carece de un enfoque preventivo, dificultando la anticipación y mitigación de riesgos relacionados con la privacidad de datos y limita la capacidad de las organizaciones para cumplir con estándares internacionales de privacidad.

Es así, que se formuló la siguiente problemática respondiendo la presente investigación: ¿Por qué se garantizará el tratamiento legítimo de datos personales mediante la incorporación del principio de Privacidad desde el Diseño en la normativa jurídica peruana? El cual se trasladó en el objetivo principal: Garantizar el legítimo tratamiento de datos personales mediante la incorporación del principio de la privacidad desde el diseño en la normativa peruana; y en los objetivos específicos: (1) Analizar la relevancia constitucional de la tutela de derecho fundamental de protección de datos personales y evaluar su impacto en el tratamiento de datos, a partir de la doctrina y jurisprudencia comparada; (2) Determinar las consecuencias jurídicas de la aplicación del principio de privacidad desde el diseño a innovaciones tecnológicas; y (3) Sustentar criterios que permitan materializar la privacidad desde el diseño como principio jurídico en el ordenamiento peruano.

En consecuencia, a la problemática planteada se formuló la siguiente hipótesis: si se incorpora la privacidad desde el diseño como principio jurídico en la normativa peruana entonces se garantizará por completo el legítimo tratamiento de datos personales. Consecuentemente da lugar al aporte que permite demostrar la hipótesis planteada con anterioridad, el cual es la: Garantizar el legítimo tratamiento de datos personales mediante la incorporación en la normativa peruana del principio de la privacidad desde el diseño.

II. Revisión de la Literatura

2.1. Antecedentes

Antes de profundizar en la exploración de teorías y conceptos, se dedicará un segmento al desarrollo de antecedentes. Esto se logrará a través de la evaluación de una amplia gama de fuentes, que incluyen tesis doctorales, de maestría y de pregrado, así como libros, revistas y artículos científicos de diversa índole

2.1.1. Investigaciones Internacionales

A partir de un enfoque internacional, tenemos como autor a Juan Bestard (2021) cuya tesis doctoral tiene por título "La gestión de datos personales y el delegado de protección de datos en la sanidad pública, con atención especial a la comunidad de Madrid", dicha investigación fue remitida a la Universidad Autónoma de Madrid, con el propósito de evaluar la implementación del Reglamento (UE) 2016/679 en el ámbito sanitario del sector público, especialmente en lo referido a la protección de los derechos digitales a cargo del delegado de protección de datos.

La relación entre este antecedente y la investigación, se basa en analizar la aplicación del Reglamento General de Datos Personales 2018/1725 de la Unión Europea para fiscalizar tratamientos de datos personales en el ámbito público de la salud, mediante la Agencia Española de Protección de Datos y como aun con la creación de un reglamento exclusivamente sobre protección de datos personales, encontramos a raíz de la pandemia falencias al resguardo del derecho fundamental a la protección de datos de carácter personal y la tesis propone un proceso de gestión de tratamientos de datos basados en los supuestos del artículo 6 que, regula el tratamiento de datos para fines compatibles y artículo 9 del Reglamento, establece las condiciones de transmisión de datos personales a destinatarios.

Dicho proceso de gestión se basa en aplicar correctamente la figura del delegado de protección de datos, quien se encarga de decidir desde el punto de vista técnico y organizativo medidas que garanticen y demuestren que el tratamiento de datos es conforme a lo establecido por ley. Este delegado no puede ser reemplazable como se ha venido realizando durante la pandemia por otras figuras de protección, puesto que, actúa como una de las garantías de la protección de tratamiento de datos.

Continuando en el mismo lineamiento internacional, hallamos en la tesis doctoral de Julio Caisa (2020) titulada "Contribución al Diseño de Sistemas Respetuosos con la Privacidad usando Patrones" presentada ante la Universidad Politécnica de Madrid. Su objetivo de estudio es brindar conocimiento de diseños de sistemas respetuosos con la privacidad aplicables en la práctica. El vínculo entre el antecedente planteado y la presente investigación, se puede advertir a raíz de los complejos escenarios de protección al derecho a la privacidad y derecho de los datos

personales en la sociedad digital actual, en consecuencia, como mecanismo utilizan el concepto de la privacidad desde el diseño adoptada por el Reglamento General de Protección de Datos Personales para fundamentar diseños de sistemas respetuosos con la privacidad, reconociendo ámbitos legales y técnicos aptos para el entendimiento del desarrollador de software.

En dichos diseños de sistemas respetuosos, la ingeniería de la privacidad toma un papel importante como figura integradora de la privacidad en el proceso de ingeniería de los sistemas, brindando teorías, técnicas, métodos y herramientas de solución. Es así, que uno de esos métodos de solución son los "patrones de privacidad", materializados en 3 tipos: lenguajes, sistemas o catálogos, aplicables por desarrolladores de software durante el ciclo de diseño de innovaciones tecnológicas para establecer controles y contramedidas o medidas de privacidad.

Finalmente, cerrando con los antecedentes internacionales está el autor Elías Grande (2021), en su tesis doctoral: "Gestión de identidades y accesos en el Internet de las Cosas" presentada a la Universidad Rey Juan Carlos. El autor, desarrolla su tesis en torno al análisis de la arquitectura del Internet *de las Cosas (LoT),* ofreciendo una propuesta para gestión de identidades, asumiendo características y limitaciones intrínsecas de los dispositivos englobados dentro del Internet de las cosas (Lot).

La aplicación práctica de la Privacidad desde el diseño, propone un mecanismo de solución para abordar las brechas de seguridad generadas por las innovaciones tecnológicas, particularmente en el contexto del Internet de las Cosas (IoT) y la principal deficiencia que se presenta en este ámbito es la falta de niveles de seguridad para verificar la autenticidad de los dispositivos IoT. En consecuencia, el mecanismo planteado plantea medidas de seguridad y privacidad destinadas al ámbito del Internet de las cosas, teniendo en consideración las restricciones inherentes a los recursos y capacidades de los dispositivos comúnmente encontrados en estos entornos.

Esta propuesta establece un sistema de gestión de identidad y acceso altamente escalable para el registro de dichos dispositivos, además de servir como cimiento para otros mecanismos esenciales que garantizan la interacción segura con servicios en la nube (tales como direccionamiento y nombrado), así como para la obtención de información compartida de manera respetuosa con la privacidad. Estableciendo un sistema de gestión de identidades y accesos que permita un registro altamente escalable de dichos dispositivos, y a su vez que sirva como base de otros mecanismos basados en interacción segura con servicios en la nube (como direccionamiento y nombrado) o obtener conocimiento colectivo de formas respetuosas con la privacidad.

2.1.2. Investigaciones nacionales

Posteriormente, hallamos como primer autor nacional a Yuriko Hidalgo (2020) como autora de la tesis de pregrado: “El paradigma del derecho global para la protección de datos personales en redes sociales”, la cual fue presentada ante la Universidad Católica Santo Toribio de Mogrovejo. La autora tuvo como objetivo crear un m mecanismo jurídico con el propósito de prevenir la utilización indebida de información personal en plataformas de medios sociales, considerando una perspectiva del derecho global.

Por tanto, la relación con el trabajo de investigación recae en la influencia de las tecnologías para la comunicación entre personas, tomando como ejemplo la interacción en redes sociales y el punto de partido para una idónea regulación de protección de datos personales es el derecho global. Pues en la actualidad la tecnología va más allá de formar parte de una interacción y empieza a determinar nuestras decisiones y parte de nuestra vida, por ende, corresponde continuar actualizando los sistemas de seguridad informáticos, sin dejar de lado la privacidad (Yuriko Hidalgo, 2020, p.13).

Es así, que propone un mecanismo jurídico enfocado a la persona, en lugar del Estado, como base para abordar esta situación desde la perspectiva del Derecho Global, dado que la sociedad está en constante cambio, el derecho también debe evolucionar y adaptarse a los nuevos acontecimientos que surgen en nuestra realidad. Esto se evidencia en el caso del Derecho Internacional, que ha tenido que adaptarse a medida que se presentaban nuevas circunstancias en cada etapa. En la actualidad, el Derecho Internacional se encuentra enfrentando una crisis debido al impacto de la globalización en nuestra sociedad.

En segundo lugar, mencionaremos al autor Salinas (2019) presentando su tesis de segunda especialidad: “La incompatibilidad existente en las obligaciones del derecho de información del titular de los datos personales”, la cual presentada ante la Pontificia Universidad Católica del Perú. Teniendo como finalidad analizar el derecho de información del titular de datos personales y las obligaciones que genera.

La relación con la temática elegida en la investigación, es el enfoque en el sector privado y el planteamiento en que la información presentada a los titulares de los datos personales, debe ser presentada de manera íntegra, y de forma sencilla. En consecuencia, surge el sistema de capas, para así impedir brechas informáticas que pueden evitarse si se cumple con el derecho de transparencia e información (Salinas, 2019, p.21).

Demostrando como la legislación actual posee un efecto -a posteriori-, se aplica cuando se incurrió en la vulneración de privacidad, más no prevé o cubre el aspecto preventivo que tutelen los datos personales, es así, que se propone el sistema de capas que consiste en 2 niveles de coordinación de información entre el titular del banco de datos personales y titular de los datos personales, con la finalidad que al titular de datos personales cuente con toda la información que asegure la integridad y sencilles del tratamiento de datos.

Finalmente concluyendo con los antecedentes nacionales, encontramos a la autora María Zamudio (2021) postulando su tesis de maestría: "El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del Sistema de Geolocalización GPS. Límites y propuestas", presentada en la Pontificia Universidad Católica del Perú, con el propósito de evaluar la ausencia de una normativa específica relacionada con la protección de datos personales y proponiendo una regulación adecuada que refuerce las salvaguardias de los empleados que están sujetos a supervisión laboral a través del uso de sistemas de posicionamiento global (GPS).

Así también, se contempla la relación con la investigación debido a que evidencia las desventajas para los trabajadores al introducir elementos tecnológicos que amplían el poder de las empresas para controlarlos, poniendo en riesgo su integridad. Esto implica una violación de derechos fundamentales, como la privacidad, por lo tanto, es necesario incorporar conceptos y medidas específicas que anticipen posibles vulneraciones

2.2. Bases Teóricas

2.2.1. Teoría del Derecho a la Autodeterminación Informativa

La teoría del derecho a la autodeterminación informativa sostiene que los individuos deben tener pleno control sobre el uso y tratamiento de su información personal. Alan Westin (1967) argumentó que la privacidad es un derecho esencial que permite a las personas decidir qué información compartir y con quién, garantizando su autonomía y protegiéndolas de abusos. Posteriormente, Daniel Solove (2021) amplió este concepto en el contexto digital, señalando que el crecimiento exponencial de las tecnologías ha generado nuevas amenazas a la privacidad, como el almacenamiento masivo de datos, el uso indebido de información personal y la vigilancia excesiva.

En el marco del *Privacy by Design*, esta teoría resulta fundamental, ya que enfatiza la necesidad de establecer medidas preventivas que aseguren que los ciudadanos mantengan el control de sus datos desde la concepción de los sistemas tecnológicos. En el caso de Perú, la Ley de Protección de Datos Personales (Ley N° 29733) reconoce este derecho, pero su eficacia

depende de que las plataformas digitales implementen principios de privacidad desde el diseño. De esta manera, no solo se cumple con la normativa, sino que se fortalece la protección de los usuarios ante posibles vulneraciones.

La aplicación de esta teoría genera beneficios significativos en el ecosistema digital. En primer lugar, fortalece la confianza de los usuarios en plataformas tecnológicas, ya que les otorga mayor transparencia y control sobre sus datos. Además, permite a las empresas y entidades cumplir con la normativa de protección de datos de manera proactiva, evitando sanciones legales y reduciendo riesgos asociados a posibles filtraciones de información.

Por el contrario, la falta de implementación de este principio puede acarrear consecuencias negativas. Sin un enfoque basado en la autodeterminación informativa, los ciudadanos quedan expuestos a usos no autorizados de sus datos, lo que puede derivar en la explotación comercial de su información sin consentimiento e incluso la manipulación de decisiones personales. Asimismo, los Estados y empresas que no garanticen este derecho pueden enfrentar crisis de reputación, sanciones regulatorias y pérdida de confianza por parte de los usuarios.

1.2.1. Teoría de la Protección Proactiva de Datos

La teoría de la protección proactiva de datos, formulada por Ann Cavoukian (2009) dentro del marco de *Privacy by Design*, establece que la privacidad debe garantizarse de manera preventiva y no solo mediante mecanismos reactivos. En este sentido, las medidas de protección deben incorporarse desde el diseño mismo de los sistemas tecnológicos, en lugar de corregir vulneraciones después de que estas ocurran. Helen Nissenbaum (2010) complementa este enfoque a través de su concepto de *privacy as contextual integrity*, el cual sostiene que la privacidad debe respetar las expectativas y normas del contexto en el que se recopilan y procesan los datos, asegurando que su uso sea legítimo y proporcional a su finalidad.

En Perú, esta teoría adquiere especial relevancia en el marco de la transformación digital de los sectores público y privado. La incorporación de la privacidad desde el diseño permite que los sistemas digitales cumplan con los principios de minimización de datos, seguridad y consentimiento informado, evitando riesgos innecesarios para los usuarios. La legislación nacional en materia de protección de datos personales se beneficia de este enfoque, ya que promueve un modelo de cumplimiento normativo basado en la prevención y en la implementación de salvaguardas técnicas y organizativas desde la concepción de las plataformas digitales.

La aplicación de esta teoría en la práctica, conlleva importantes beneficios tanto para los usuarios como para las organizaciones. En primer lugar, permite reducir de manera significativa las brechas de seguridad y la exposición de datos personales a ataques cibernéticos, ya que las

medidas de protección están integradas desde la fase de desarrollo de los sistemas. Asimismo, contribuye a generar confianza en el entorno digital, al garantizar que las plataformas tecnológicas operen con estándares adecuados de privacidad y seguridad.

Sin embargo, la ausencia de este enfoque puede traer consecuencias perjudiciales. Si las empresas y entidades gubernamentales no implementan principios de protección proactiva, aumentan las probabilidades de sufrir filtraciones de datos masivas, con los consiguientes daños a los derechos de los ciudadanos. Además, la ausencia de un enfoque de privacidad desde el diseño puede derivar en sanciones legales, pérdida de reputación y desconfianza generalizada en el uso de servicios digitales, lo que dificulta la evolución del ecosistema tecnológico del país.

Las teorías relacionadas con el derecho a la autodeterminación informativa y de la protección proactiva de datos, representan pilares fundamentales para interpretar y respaldar el principio de "Privacidad desde el Diseño" en el contexto del tratamiento de datos personales en el Perú. Ambas corrientes subrayan la relevancia de salvaguardar la privacidad de forma preventiva, garantizando que las personas conserven el control sobre su información personal y que las entidades incorporen mecanismos de seguridad desde la concepción de sus sistemas tecnológicos.

El aporte de estas teorías a la investigación radica en su capacidad para evidenciar que la privacidad no debe ser concebida como una reacción ante vulneraciones, sino como un elemento inherente al desarrollo de cualquier plataforma digital. Su influencia permite comprender la necesidad de diseñar marcos normativos y estrategias empresariales que prioricen la seguridad de los datos desde el inicio, reduciendo riesgos y fortaleciendo la confianza de los ciudadanos en el entorno digital. De esta manera, la aplicación del *Privacy by Design* no solo se convierte en una obligación legal, sino en un mecanismo clave para garantizar una protección efectiva y sostenible de la información personal en la era tecnológica.

2.3. Bases Conceptuales

2.3.1. Derecho Fundamental de Protección de Datos Personales

Regulación Constitucional del derecho fundamental de Datos Personales Las bases jurídicas que protegen y reconoce el derecho a la protección de datos personales en nuestro país surge en 1993 con la vigencia de la Constitución Política del Perú, en el artículo 02 inciso 06 prescribe "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" (1993).

Asimismo, el NCPC, va más allá de la conceptualización y determina los límites del derecho a la autodeterminación informativa, creando las bases para establecer garantías jurídicas que protejan los datos personales de las personas, quienes poseen la opción de recurrir al

procedimiento de hábeas data con el fin de: "Reparar agresiones derivadas del manejo indebido de datos sumamente personales registrados en sistemas de información, ya sean digitales o físicos. Asimismo, permitir el acceso y control sobre el uso que se le está dando a dicha información (…)" (artículo 59 NCPC). Reconociendo constitucionalmente lo que internacionalmente se denomina derechos ARCO – Acceso, Rectificación, Cancelación y Oposición, correspondientes a los titulares de datos personales.

Como autores clásicos referentes del estudio del derecho a la privacidad, destacamos a Warren y Brandeis quienes, en 1980, desarrollaron el significado de privacidad en el artículo denominado "El derecho a la Privacidad", dicho estudio aún adquiere relevancia por la propuesta que establece "la protección de la persona es un principio fundamental en el ámbito jurídico que, de manera ocasional, requiere una nueva definición en términos de su naturaleza y la amplitud de la protección que conlleva" (Warren y Brandeis, 1890). De tal forma, cada individuo tiene la potestad de determinar en qué medida comparte sus pensamientos, sentimientos y emociones con los demás.

Posteriormente, con la publicación del articulo "Privacidad" de William Prosser quien, en términos vinculados y aplicables al sistema legal estadunidense, permitió su viabilidad, determinando la lesión de la privacidad como "lo cual puede manifestarse a través de: i) el acceso no autorizado; ii) la exposición pública de aspectos íntimos; iii) la difusión de contenido que distorsiona la identidad de una persona; y, iv) el uso indebido del nombre o la imagen de un individuo" (Prosser, 1960, 320 p.). Es así que, aunque no puede ser impecable sus clasificaciones de daños han proporcionado una valiosa base conceptual permitiendo en el marco de la responsabilidad civil la adopción de la protección de los datos personales.

2.3.1.1. Legislación sobre Protección de Datos Personales

Las bases constitucionales planteadas con anterioridad, permitieron 08 años después de su resolución, construir una normativa reactiva, materializada en la Ley N° 29773, Ley de Protección de Datos Personales en el 2011, teniendo en cuenta los derechos otorgados al individuo que posee datos personales, ya sea en relación con una organización pública o privada, para obtener información (derecho de acceso) sobre qué datos personales se están procesando y actualizar cualquier información que no refleje adecuadamente la situación actual del titular.

El objetivo de la Ley de Protección de datos personales es "garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú" (p.02, 2011). Tutelando el resguardo de incorporar toda información

pertinente y necesaria para el propósito original de recolectar los datos.

2.3.1.2. Desarrollo Jurisprudencial

En el año 2002 con la sentencia del Tribunal Constitucional N° 01797-2002-HD/TC, denomina la protección de datos personales como el derecho a la autodeterminación informática, señalando que "ingresar a los archivos de información, ya sean digitales o físicos, sin importar su tipo o naturaleza, donde se encuentren almacenados los datos personales de un individuo. Este acceso tiene como finalidad conocer el contenido registrado, su propósito, el destinatario de dicha información, así como identificar a quienes recopilaron esos datos." (TC,2003).

Asimismo, las demandas que exigen su reconocimiento están frecuentemente vinculadas a la protección de más derechos constitucionales, como: El derecho a la identidad personal, imagen y privacidad, entre otros, el derecho a la autodeterminación informática se considera un derecho fundamentado que permite ejercer control sobre el almacenamiento, divulgación y uso de datos personales. Asimismo, encontramos otros derechos vinculantes como:

El derecho a la intimidad, reconocido en la Constitución Política, dado que este derecho salvaguarda el derecho a la privacidad, es decir, la facultad jurídica de rechazar intromisiones indebidas en la vida privada o familiar de las personas se complementa con la autodeterminación informativa, la cual asegura que cada individuo tenga la capacidad de salvaguardarla al tener control sobre el registro, uso y revelación de los datos relacionados con ellos.

El derecho a la imagen tiene como objetivo principal amparar la reputación de las personas, la cual se deriva de su dignidad inherente. Por otro lado, el derecho a la autodeterminación asegura que el individuo posee capacidad de controlar y decidir qué datos se registran sobre él, con el propósito a la presentación pública de la personalidad de alguien no sea perturbada ni distorsionada debido asegurar la atribución de ideas, opiniones o comportamientos que difieren de los expresados por la persona en su vida social.

Estos constituyen algunos derechos correlacionados con la tutela de datos personales, en ese sentido, el TC sostuvo que "los datos personales pueden estar asociados a cualquier esfera de la vida del individuo; y, dependiendo del tipo de dato que sea tratado de forma inadecuada, podría verse vulnerado no solo el derecho a la autodeterminación informativa, sino también uno o varios derechos adicionales" (Zamudio, p.344,2020).

2.3.1.3. Mecanismos de Protección Nacionales para el legítimo Tratamiento de Datos

Actualmente en el Ordenamiento Peruano, no contamos con instancias superiores, a las

cuales, recurrir cuando se realice una lesión al derecho de protección de datos personales. Sin embargo, el Ministerio de Justicia y Derechos Humano creo una institución sancionadora denominada Autoridad Nacional de Protección de Datos Personales (en adelante ANPD), encargada de sancionar toda infracción de la Ley N° 29733 de Protección de Datos Personales.

Esta organización, cuenta con dos unidades orgánicas: Dirección de Protección de Datos Personales, encargada de resolver los procedimientos sancionadores sobre protección de datos personales, y la Dirección de Fiscalización e Instrucción, "responsable de fiscalizar el cumplimiento de las obligaciones y prohibiciones establecidas en la Ley de Protección de Datos Personales y su Reglamento, así como de iniciar los procedimientos sancionadores por infracción a las disposiciones sobre Protección de Datos Personales e instruir el procedimiento sancionador" (Ministerio de Justicia y Derechos Humanos, p.11, 2015).

La ANPD trabaja bajo los lineamientos de los derechos ARCO – Acceso, Rectificación, Cancelación, Oposición-, estos derechos se encuentran regulado por la Ley de Protección de Datos Personales peruana y se basa en otorgarles potestad a las personas de controlar su información personal, con la finalidad de salvaguardar el derecho a obtener la información de sí mismo, de solicitar la corrección de información que sea parcial o totalmente inexacta, incompleta, errónea o falsa, como suprimir información personal, permitiendo al titular de datos personales solicitar la eliminación o cancelación de sus datos de una base de datos personal cuando ya no sean necesarios o pertinentes para la finalidad para la cual fueron recopilados.

2.3.1.4. Sanciones Nacionales: Caso N° 396-2023-JUS/DGTAIPD-DPDP

La Resolución Directoral N° 396-2023, fue emitida por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, analizó la responsabilidad administrativa del Banco BBVA Perú, en relación a la infracción del reglamento de la Ley de Protección de Datos Personales, por utilizar datos personales para comunicarse telefónicamente con el denunciante, con fines comerciales.

La resolución de sanción buscó advertir y comprobar si se llegaron o no a transgredir los artículos de la LDPD para justificar la infracción y aplicar la sanción correspondiente. En el caso analizado, se acreditó la vulneración del artículo 5 de la Ley de Protección de Datos Personales (LPDP), el cual establece que "el tratamiento de datos personales requiere el consentimiento del titular". En consecuencia, también se transgredió el artículo 13.5 de la misma norma, que regula el alcance del tratamiento de dichos datos, al disponer que "los datos personales solo pueden ser tratados con el consentimiento del titular, salvo que una ley lo autorice expresamente. Dicho consentimiento debe ser previo, informado, explícito e

inequívoco".

Se advierte entonces que, el titular de datos personales ya no desea el tratamiento de sus datos, el cual había otorgado previamente, sin embargo, ya no existe un consentimiento válido que justifique dicho procesamiento, incurriendo en una infracción y dando como resultado, la emisión de la resolución que declara sancionar al Banco BBVA con una multa, por el procesamiento de datos personales del denunciante con fines comerciales y publicitarios sin el consentimiento respaldado legalmente, por la revocación del consentimiento y garantizando los antes mencionados derechos ARCO, que posee el titular de datos personales.

2.3.1.5. Mecanismos de protección Internacionales del tratamiento de datos personales

Dentro del marco europeo, el Reglamento General de Protección de Datos (en adelante RGPD) es una legislación establecida por el Parlamento Europeo y el Consejo en 2018. Esta normativa se considera fundamental para proteger los derechos fundamentales de las personas en la actualidad y fomentar la actividad económica al brindar claridad sobre las regulaciones aplicables al sector público y privado en el mercado digital.

En aplicación del Reglamento mencionado, se creó el Comité Europeo de Protección de Datos, integrado por representantes de las autoridades nacionales de protección de datos de los Estados miembros de la UE/EEE, junto con el Supervisor Europeo de Protección de Datos. Este organismo tiene como finalidad emitir directrices sobre los principios esenciales del RGPD y de la Directiva en materia penal, asesorar a la Comisión Europea respecto a cuestiones relacionadas con la protección de datos personales y con nuevas propuestas legislativas dentro de la Unión Europea, así como resolver de manera vinculante los conflictos que surjan entre las autoridades nacionales de control.

España ocupa una posición destacada con respecto a regulación de los datos personales porque cuenta con la Agencia Española de Protección de Datos (AEPD), una autoridad pública creada mediante Ley Orgánica 5/1992, de 29 de octubre. La Agencia fue constituida para ser independiente, pero colabora con el Consejo del Poder de Justicia, para garantizar el correcto desempeño de los lineamientos que les confiere la Ley Orgánica de 1985, bajo "la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos" (Morales, p.179,2022).

2.3.1.6. Caso: Google vs AEPD C- 131/12

La sentencia del Tribunal de Justicia de la Unión Europea, analiza la controversia del derecho al olvido dentro del Internet, pues de 13 de mayo de 2014, admitió el derecho frente a los buscadores de Internet. Tras este fallo, la historia de Internet experimentó un cambio

significativo, ya que su influencia no se limita únicamente a salvaguardar los derechos fundamentales de los usuarios, como la privacidad y la protección de sus datos personales, sino que también ha llevado al necesario rediseño de los servicios más populares de Internet, como los motores de búsqueda y las redes sociales.

El caso abordó la cuestión de si los motores de búsqueda en Internet están obligados a eliminar enlaces de sus resultados, incluso cuando el nombre o los datos personales no han sido previamente ni simultáneamente retirados de las páginas web que los contienen, y aun cuando dichas publicaciones sean legalmente válidas. Esto obedece a que cualquier usuario que realice una búsqueda utilizando el nombre de una persona puede acceder, mediante los resultados ofrecidos, a una recopilación organizada de información sobre dicha persona disponible en línea, lo que facilita la elaboración de un perfil más o menos detallado del individuo consultado.

Finalmente, la sentencia del Tribunal emitida en el litigio entre Google España y la Agencia Española de Protección de Datos, concluyó que "la actividad de un motor de búsqueda, consistente en localizar información publicada en Internet por terceros, indexarla automáticamente, almacenarla de forma temporal y, posteriormente, ponerla a disposición de los usuarios según un determinado orden de relevancia, implica que el operador del motor de búsqueda debe ser considerado como «responsable» del tratamiento de dichos datos" (Sentencia del Tribunal de Justicia de la Unión Europea, p.22).

En consiguiente, el Tribunal solicita que, si la información en cuestión ya no está disponible para el público en general a través de su aparición en los resultados de búsqueda, los derechos individuales tienen prioridad sobre el interés económico del motor de búsqueda y también sobre el interés del público en acceder a dicha información al buscar el nombre de esa persona. No obstante, esta circunstancia puede variar en situaciones específicas, especialmente cuando la persona en cuestión cumple un rol significativo en la vida pública. En tales casos, la intromisión en sus derechos fundamentales podría considerarse justificada debido al interés prevalente del público en acceder a dicha información a través de los resultados de búsqueda.

2.3.2. El Principio de Privacidad desde el diseño en Innovaciones Tecnológicas

2.3.2.1. Origen de la Privacidad desde el diseño

Se desarrolló el concepto de Privacidad desde el Diseño (en adelante PdD) en el evento Privacy by Design: The Definitive Workshop en la década de 1990, destacando por plantear como a medida que la tecnología de la información evolucionaba, la interconexión y el volumen de información personal recopilada podría comenzar a saturarse, quedando claro que se necesitaba una nueva forma de pensar sobre la privacidad (Cavoukian, 2010).

El término PdD fue contemplado por primera vez en el informe creado por la Autoridad

Holandesa de Protección de Datos y el Comisionado de Información de Ontario titulado *Tecnologías de mejora de la privacidad: el camino hacia el anonimato,* publicado en 1995. Dicho informe, "exploró un nuevo enfoque para la protección de la privacidad, con una serie de estudios de casos que muestran que los sistemas sin datos personales (o al menos con muchos menos datos personales) podrían tener las mismas funcionalidades" (Hunstinx, P., p.254, 2010).

En consecuencia, la PdD es una medida proactiva, materializada en la configuración de las innovaciones tecnológicas, debido que su objeto es evitar que se realicen infracciones de privacidad (Cavoukian, 2010). Este concepto incluye prácticas sólidas de privacidad, durante el tiempo de vida de las innovaciones tecnológicas y pueden ser tanto colectivas como individuales "el carácter colectivo de la privacidad se evidencia en que, primeramente, los datos relativos a un individuo con frecuencia comprenden información sobre otros (verbigracia, los datos genéticos). Adicionalmente, los efectos perjudiciales de las filtraciones de privacidad a menudo se padecen de forma individual." (Veliz, 2021, p. 433).La PdD, se enfoca en la configuración de la privacidad antes de la creación o hecho, ambientada en la construcción de innovaciones tecnológicas previniendo eventos invasivos de privacidad, pues este concepto tomado como principio tiende a garantizar el tratamiento legítimo de datos personales en el ordenamiento jurídico peruano, a través de la minimización de datos durante la etapa de la configuración de tratamiento.

Del mismo modo, aparecen críticos que cuestionan la efectividad o materialización en la realidad de la PdD porque "la definición actual de PbD no aborda el aspecto metodológico de la ingeniería de sistemas, es decir, no detalla los métodos de ingeniería de sistemas utilizados. Estos métodos deben cubrir todas las especificaciones técnicas del sistema y el ciclo de vida de los datos" (Palacios, D., Cousid, MP, y otros; p. 218; 2022).

No obstante, la Agencia Española de Protección de Datos en 2019, con la publicación de la Guía de Privacidad desde el diseño (en adelante GPD), prevé este escenario, porque no podemos olvidar que la mitigación de riesgos se encuentra integrada a la concepción de la privacidad desde el diseño y mediante la guía, se postula la figura de "la ingeniería de la privacidad" encargada de traducir las concepciones de la privacidad en términos prácticos y operativos que permitan su materialización en el ciclo de vida de los sistemas de información, aplicadas por profesionales de datos personales, organizaciones, empresas, desarrolladores de software, o todo interesado que maneje, procese o tenga interacción con datos personales.

La PdD, se originó como un enfoque proactivo para garantizar que la privacidad esté presente en todas las etapas de desarrollo de sistemas, productos, servicios y procesos que involucran

datos personales, con el objetivo de salvaguardar la información personal ante la creciente preocupación por la protección de datos personales en un mundo cada vez más digital.

2.3.2.2. Principios Fundacionales de la Privacidad desde el Diseño

Ann Cavoukian, plantea siete principios fundacionales de la Privacidad desde el Diseño, basándose en los principios de Practicas Justas de información creadas por el Departamento de Seguridad de Estados Unidos, para argumentar la aplicación de la privacidad como un modelo estándar, estos son: (1) Proactivo, no reactivo; preventivo, no correctivo, (2) Privacidad como configuración predeterminada, (3) Privacidad incorporada en la fase de diseño, (4) Funcionalidad Total: pensamiento "todos ganan", (5) Aseguramiento de la privacidad en todo el ciclo de vida, (6) Visibilidad y transparencia; y, (7) Respeto por la privacidad de los usuarios

Estos principios fundamentan la operatividad de la PdD como un enfoque preventivo, al "adelantarse a los acontecimientos que puedan impactar la privacidad antes de que ocurran" y al integrarse de manera esencial e inseparable en los sistemas, aplicaciones, productos y servicios, así como en las prácticas comerciales y los procesos de la organización. (Guía de la Privacidad desde el Diseño, p.10, 2019). Todo esto, sin dejar la transparencia como un elemento clave para evidenciar la diligencia en el tratamiento de datos y la responsabilidad proactiva ante la autoridad de control. El objetivo final es asegurar los derechos y libertades de los usuarios, quienes deben tener la facultad de administrar su propia información.

2.3.2.3. Enfoque metodológico entre gestión de riesgos y la responsabilidad proactiva

Según el Foro Económico Mundial (2020) en el "Reporte de Riesgos Mundiales", se advierte el incremento significativo de ataques cibernéticos en un 75%, específicamente en robo de datos personales a nivel mundial y como en el 2021 los delitos por ciber crimen podrían alcanzar los 6 billones de dólares, equivalente al PBI de la tercera economía más grande del mundo. En consecuencia, las brechas de seguridad siempre continuarán sucediendo, puesto que los softwares continuamente serán actualizados para incurrir en ataques cibernéticos.

Y una vez identificado el tipo de riesgo, aparece la gestión de riesgos, que es "el proceso de cómo tomar decisiones en función de los riesgos. Es un enfoque sistemático para entender el entorno de riesgos y para establecer criterios apropiados que permitan a los directores tomar decisiones informadas" (Pritchard, C. ,2014). Este enfoque dentro de la privacidad desde el diseño, está orientado a identificar, evaluar y mitigar los riesgos relacionados con la privacidad, teniendo como objetivo minimizar la probabilidad de que ocurran eventos no deseados o minimizar su impacto en caso de que se materialicen.

El desarrollo de la PdD, en la normativa europea, involucra la participación activa de la gestión de riesgos, pues la utiliza como planteamiento dinámico de mejora continua para entender los riesgos a la privacidad y determinar las medidas técnicas y organizativas a implantar de acuerdo a la complejidad de cada innovación tecnológica creada o por crear. Su rol principal es establecer estrategias concretas a lo largo del ciclo de vida de las innovaciones tecnológicas, materializadas en los sistemas, softwares, proceso tecnológicos o servicios, durante todas las fases de desarrollo de la misma hasta su retirada, con el objetivo que la protección de los datos personales nunca sea vulnerada (Agencia Española de Protección de Datos, 2019).

Este enfoque garantiza la protección proactiva de la privacidad y el cumplimiento normativo, construyendo confianza y reduciendo los riesgos asociados con la recopilación y el procesamiento de datos personales, mediante un proceso que involucra, la identificación de riesgos para la anticipación de posibles amenazas, el análisis de información detallada sobre su probabilidad e impacto, el control de la implementación de medidas de mitigación, y el seguimiento y revisión aseguran que las estrategias de gestión de riesgos sigan siendo efectivas a lo largo del tiempo.

Paralelamente, también se involucra como garantía de la privacidad desde el diseño, el cumplimiento de responsabilidad proactiva, que es un principio utilizado a nivel mundial para consolidar la responsabilidad y obligación de las organizaciones o encargados de la protección de la privacidad en el tratamiento de datos personales, señalando “que el responsable debe definir desde el inicio una estrategia para demostrar la implementación de medidas efectivas que aseguren el cumplimiento de la normativa sobre el Tratamiento de Datos Personales.” (Londoño, 2021, p.32). Es decir, establece que el responsable del tratamiento de datos debe garantizar y demostrar el cumplimiento de la normativa, implicando adoptar medidas técnicas y organizativas adecuadas para proteger los datos personales y minimizar los riesgos de violación de la privacidad.

La responsabilidad proactiva, en la PdD, es entendida como un autoanálisis crítico, continuo y rastreable del responsable del tratamiento en el cumplimiento de las obligaciones que le exige la normativa. Este principio tiene como finalidad garantizar en la practica la efectividad del tratamiento de datos, puesto que exige la responsabilidad de las organizaciones y encargados, a través del cumplimiento real y efectivo de las funciones correspondientes (Remolina & Álvarez, 2018).

Sin embargo, este principio también ha sido objeto de críticas que señalan sus posibles limitaciones y desafíos, al considerarlo difícil de aplicar en la práctica, ya que requiere una evaluación continua y dinámica de los riesgos y las medidas de protección, así como una documentación exhaustiva y actualizada de los procesos y procedimientos relacionados con el tratamiento de datos, llegando a ser considerada "igual de útil o de inútil que las leyes, si en la práctica, las organizaciones no hacen nada para cumplir uno u otro". Por consiguiente, los resultados que se esperan de su aplicación dependerán del nivel de compromiso y la formalidad con que la organización concrete en el tratamiento de datos lo establecido en las normativas, e incluso implemente acciones proactivas que añadan valor. (Remolina & Álvarez, p.29, 2018).

La responsabilidad proactiva es un principio clave del RGPD, que establece la responsabilidad de garantizar y demostrar el cumplimiento de la normativa, y su importancia radica en las consecuencias que genera su cumplimiento pues, ayudará a las organizaciones a evitar sanciones administrativas por incumplimiento del RGPD, también al adoptar medidas técnicas y organizativas adecuadas, las organizaciones pueden mejorar su capacidad para detectar, prevenir y mitigar los riesgos asociados al tratamiento de datos personales, lo que a su vez puede mejorar la confianza y la satisfacción de los interesado.

Asimismo, el vínculo entre la gestión de riesgos y responsabilidad proactiva, son las prácticas para proteger la privacidad de los individuos y garantizar que las organizaciones operen de manera ética y cumplan con las regulaciones de protección de datos, ambos enfoques son necesarios para abordar los riesgos de privacidad de manera efectiva y sostenible.

Es así como la suma integral del enfoque de la gestión de riesgos y la responsabilidad proactiva son la esencia de la Privacidad desde el diseño, pues a través de la gestión de riesgos es que puede realizarse la configuración de la privacidad durante el ciclo de vida de las innovaciones tecnológicas y la responsabilidad proactiva otorga el carácter obligatorio que requiere el principio para garantizar la protección de datos personales.

2.3.2.4. Estrategias de Diseño de la Privacidad en innovaciones tecnológicas

El desarrollo masivo de la tecnología ha llegado a ser catalogado en la actualidad como la Industrial 4.0, “las Tecnologías de la Información y la hiperconectividad son pilares fundamentales para la sociedad. De esta manera, el entorno digital ha ganado una gran importancia social y jurídica, transformando la sociedad del siglo XXI.” (Muñoz, J; p. 08 ;2019).

Es decir, la Industria 4.0 representa la digitalización del sector industrial a través de la incorporación de tecnologías avanzadas como el internet de las cosas, la inteligencia artificial, el big data, la robótica y la impresión 3D. Sus ventajas principales incluyen el aumento de la

productividad, la eficiencia y la calidad de los procesos, la mejora de la seguridad laboral, la toma de decisiones fundamentada en datos, el incremento de la competitividad y la optimización de la rentabilidad a mediano y largo plazo.

A partir, de este contexto surgen innovaciones tecnológicas aún más disruptivas que implican el almacenamiento de datos personales. Por ello, la valoración constante y adaptable de los riesgos y las medidas de protección de la privacidad desde la concepción misma de estas tecnologías resulta fundamental para salvaguardar de manera proactiva el derecho fundamental a la protección de datos.

2.3.2.5. Innovación tecnológica: Internet de las Cosas

Cuando surge la Industria 4.0, se desglosa la integración de El internet de las cosas o Internet of Thing (IoT) que es una herramienta de interconexión digital de dispositivos cotidianos con internet, "como heladeras, licuadoras, impresoras, automóviles, iluminación y en general cualquier aparato que interactúe de alguna forma con una persona" (Zito,M, p.38,2018). Estos dispositivos cotidianos logran ser "inteligentes" al comunicarse, recopilar datos y tomar decisiones de manera autónoma a través de sensores, redes inalámbricas y sistemas de información, de acuerdo a la funcionalidad por la cual fue creada.

Sin embargo, desde 2018 ha incrementado un 29% los ciberataques y "los dispositivos IoT se consideran de alto riesgo dado que pueden causar daños físicos y poner en peligro la vida de una persona" (Silva,A; Heredia,J; Arjona,P; Juárez,A & Sandoval,A; p.316, 2019). Su funcionalidad abarca diversas industrias y puede incluir monitoreo de pacientes en tiempo real en la atención médica, optimización de cadenas de suministro en la logística, gestión eficiente de recursos en la agricultura, y sistemas de control de edificios y tráfico en las ciudades inteligentes, entre otras. Por tanto, la privacidad juega un papel importante en la red de inteligencia que involucra los IoT, es así que, mediante el área encargada de obtener patrones sobre posibles brechas de seguridad, se crea estrategias defensivas que protegen futuras vulneraciones de privacidad, configurándose la protección de datos personales durante el ciclo de vida de las IoTs.

Una de las herramientas que permiten obtener los anteriormente mencionados patrones son los medidores inteligentes, son instrumentos fundamentales para identificar patrones de consumo, ya que facilitan la comunicación bidireccional entre usuarios y empresas de servicios. "Dada su operación automatizada y la precisión de la información que generan, los datos de estos medidores pueden revelar detalles significativos sobre las actividades y conductas de los usuarios al ser analizados con técnicas de minería de datos" (Silva,A; Heredia,J; Arjona,P; Juárez,A & Sandoval,A; p.318, 2019).

Es así que, la PdD se puede configurar en el Internet de las cosas, el cual mediante patrones garantiza que los sistemas y dispositivos IoT respeten y protejan la privacidad de los usuarios desde el principio de su desarrollo y a lo largo de su ciclo de vida, buscando evitar posteriores lesiones en la privacidad y reducir los riesgos asociados con la recopilación, el procesamiento y el almacenamiento de datos personales por parte de dispositivos IoT.

III. Materiales y Métodos

La presente investigación se enmarca según el análisis documental, Bernal (2016) define esta técnica como el estudio de material impreso mediante fichas bibliográficas (p. 194). En otras palabras, este procedimiento se aplica a fuentes documentales importantes para desarrollar los argumentos y alcanzar los objetivos de la investigación. Por lo tanto, implica un trabajo intelectual de extracción, donde se recopilan conceptos clave y sintéticos de las fuentes originales, facilitando su consulta y la creación de nuevos documentos.

Asimismo, es importante destacar el carácter cualitativo de la investigación, por tener un impacto significativo en el procedimiento de tratamiento de datos personales en el Perú y la mejora de prácticas que acarrearía la aplicación del principio planteado en la investigación, esto utilizando el método analítico que busca hacer una descomposición del objeto de estudio en sus elementos constitutivos o dimensiones, aplicando este proceso también sobre la información recuperada de las distintas fuentes consultadas, atendiendo a cualquier similitud o divergencia entre las teorías y, por consiguiente, concluyendo a través de una propuesta con un basamento argumentativo suficiente (Campos, 2017). Por lo tanto, en esta investigación se seguirá el método analítico, debido a que toda propuesta teórica será puesta bajo examen en consonancia con los objetivos perseguidos en este trabajo investigativo.

IV. Resultados y Discusión

La presente investigación pretende bajo el análisis constitucional fundamentar la protección y legítimo tratamiento del derecho fundamental de datos personales, mediante la incorporación de la Privacidad desde el Diseño como principio jurídico en la normativa peruana.

4.1. Análisis de la relevancia constitucional de la tutela del derecho fundamental de protección de datos personales y evaluar su impacto en el tratamiento de datos

En este apartado, analizaremos junto a la doctrina y jurisprudencia comparada europea, el reconocimiento constitucional de la protección de datos personales en el ordenamiento peruano y contemplamos a través de autores clásicos como Warren y Brandeis, el significado de privacidad en su artículo publicado “El derecho a la Privacidad”, por la propuesta que establece “la protección de la persona es un principio fundamental en el ámbito jurídico que, de manera ocasional, requiere una nueva definición en términos de su naturaleza y la amplitud de la

protección que conlleva" (Warren y Brandeis, 1890). Proporcionando en el marco de la responsabilidad civil la adopción de la protección de datos personales, el cual, continúa evolucionando y adaptando medidas de protección de acuerdo a las necesidades de cada estado.

4.1.1. Reconocimiento constitucional de la protección de datos personales como derecho fundamental

El derecho fundamental a la protección de datos personales, es reconocido desde el derecho constitucional sustantivo y adjetivo en el Perú, adquiriendo con el tiempo mayor protagonismo desde la Constitución de 1993, pues la finalidad es proteger la dignidad de las personas y se advierte que los datos personales se encuentran correlacionados con otros derechos fundamentales como el derecho a la intimidad, a la imagen, entre otros, es decir, la vulneración a los datos personales repercute en los demás derechos antes mencionados, en consecuencia su protección es inminente, conforme lo señala Zamudio (2020) pues "Los datos personales abarcan diversos aspectos de la vida de una persona; su tratamiento indebido puede vulnerar tanto el derecho a la autodeterminación informativa como otros derechos fundamentales." (p.344).

Actualmente el incremento masivo de innovaciones tecnológicas que funcionan en base al tratamiento de datos personales requiere un mayor blindaje, y en ese lineamiento el NCPC, solidifica la apertura de los ciudadanos a acudir al proceso de habeas data a fin de "reparar agresiones contra la manipulación de datos personalísimos almacenados en bancos de información computarizados o no. A conocer y supervisor la forma en que la información personal viene siendo utilizada (…)" (art.59).

Cabe resaltar, que también tiene un reconocimiento jurisprudencial, manifestado en la sentencia del Tribunal Constitucional N° 01797-2002-HD/TC, que denomina la protección de datos personales como autodeterminación informativa, y advierte el ejercicio de poder del titular de datos personales, quien decide sobre la información recopilada, registrada o almacenada en bases de datos, archivos o registros de diversa índole que estén bajo la gestión de entidades tanto públicas como privadas. Porque la autodeterminación informativa, es crucial para la protección de los derechos individuales y la privacidad de las personas, al establecer que las personas tienen el derecho de decidir qué información personal comparten y cómo se utiliza, y su importancia radica en la protección de la dignidad humana y la prevención del abuso de datos personales.

Finalmente, si bien el reconocimiento constitucional del derecho a la protección de datos personales inicia con la Constitución de 1993, es mediante el NCPC que se complementan los derechos correspondientes al titular de datos personales frente a una institución pública o privada y la sentencia del Tribunal Constitucional N° 01797-2002-HD/TC, recalca la

importancia que requiere su protección al estar correlacionados con otros derechos, sin embargo, surge la interrogante de porque aún con las garantías constitucionales, en el Perú no contamos con jurisprudencia en instancia superiores que nos brinde un mayor alcance o análisis de este derecho fundamental, pues en la actualidad contamos solo con sanciones administrativas.

4.1.2. Mecanismos de Protección para el legítimo tratamiento de datos personales mediante jurisprudencia comparada

En este apartado, se analizan las medidas de protección de datos personales utilizadas en el Ordenamiento Peruano, y como 11 años después de su reconocimiento constitucional, se construyó una normativa reactiva, estableciendo principios, derechos, obligaciones y sanciones para regular el tratamiento de datos personales por parte de los titulares de derecho y los encargados de los bancos de datos, más no cuenta con una regulación proactiva que prevea posibles brechas de seguridad, a pesar que estas son imposibles de evitar porque el mundo continuara tecnificándose y a la par se creara más métodos de cyber ataques, a eso sumémosle la deficiencia q contiene la LPDP al no contar con herramientas de prevención.

Aun así, el foco de la LPDP continúa centrado en concretar mecanismos de protección posterior a la vulneración del derecho de datos personales, es así como, se instituye la Autoridad Nacional de Protección de Datos Personales (en lo sucesivo, ANPD) como la entidad con potestad sancionadora en el ámbito de la protección de datos personales. Dicha organización se articula a través de dos dependencias orgánicas: la Dirección de Protección de Datos Personales, a la cual compete la resolución de los procedimientos sancionadores relativos a la protección de datos personales, y la Dirección de Fiscalización e Instrucción, “responsable de supervisar el cumplimiento de las obligaciones y prohibiciones prescritas en la LPDP y su Reglamento, así como de incoar los procedimientos sancionadores pertinentes” (Ministerio de Justicia y Derechos Humanos, p.11, 2015).

La ANPD, a través Resolución Directoral N° 396-2023, analiza la responsabilidad administrativa del Banco BBVA Perú ante la infracción del reglamento de LPDP por utilizar datos personales para comunicarse telefónicamente con el denunciante, con fines comerciales. La resolución de la sanción es advertir y comprobar si se llegan o no a transgredir los artículos de la LDPD para justificar la infracción y sanción correspondiente si es que fuera ello o no, y en el presente caso se comprobó la infracción y se sanciono la entidad bancaria.

Paralelamente, dentro del marco europeo, el Parlamento Europeo y el Consejo establecieron en 2018 el Reglamento General de Protección de Datos (RGPD). Asimismo, resalta la Agencia

Española de Protección de Datos (en adelante AEPD), una autoridad pública autónoma creada por la Ley Orgánica 5/1992, de 29 de octubre. Esta normativa y entidad se consideran cruciales para la protección del derecho fundamental a los datos personales. El RGPD unifica las regulaciones de protección de datos en toda la Unión Europea y, a través de la AEPD, asegura su cumplimiento por parte de las empresas que operan en diversos países de la UE. La AEPD no solo supervisa las obligaciones del estado y las empresas en el tratamiento de datos personales y los derechos de los titulares, sino que también promueve la concienciación pública, convirtiendo a ambos en un mecanismo eficaz para la protección de datos personales en la era digital.

Sin embargo, a raíz de la pandemia, se hicieron evidentes las deficiencias de este sistema que, en apariencia, cubre todos los aspectos relacionados con la protección de datos personales, desde la configuración de innovaciones tecnológicas que los contienen y su tratamiento, hasta la finalización de su uso. Así lo señala Juan Bestard (2021) en su tesis doctoral "La gestión de datos personales y el delegado de protección de datos en la sanidad pública, con atención especial a la comunidad de Madrid", presentada a la Universidad Autónoma de Madrid. En su análisis del desempeño del Reglamento (UE) 2016/679 en el sector público de la salud, Bestard observa que, a pesar de la creación de una normativa específica sobre protección de datos personales, persisten fallas en la salvaguarda de este derecho fundamental. En consecuencia, la tesis propone complementar la gestión de tratamientos de datos estableciendo las condiciones para la transmisión de datos personales a destinatarios.

La relevancia que posee el AEPD y el RGPD, se refleja con la sentencia del 13 de mayo del 2014, Google vs AEPD C- 131/12 del Tribunal de Justicia de la Unión Europea, pues tras el fallo de advertir el derecho al olvido frente a los buscadores de Internet, la historia de Internet experimentó un cambio significativo, ya que su influencia no se limita únicamente a salvaguardar los derechos fundamentales de los usuarios, como la privacidad y la protección de sus datos personales, sino que también ha llevado al necesario rediseño de los servicios más populares de Internet, como los motores de búsqueda y las redes sociales.

Por último, se identifica una deficiencia en la regulación de los datos personales en el Perú, al solo poseer una entidad sancionadora, la ANPD, que analiza la responsabilidad administrativa de la posible infracción, no obstante, actualmente no contamos con instancias superiores, a las cuales, recurrir cuando se realice una lesión al derecho de protección de datos personales, todo proceso se quede en instancias administrativas, a diferencia de Europa que cuenta con un

mecanismo de protección más completo, que se encuentra en continuo mejoramiento y posee instancias superiores a las cuales recurrir cuando se vulnera el derecho fundamental de la protección de datos personales tal como el Tribunal de Justicia de la Unión Europea.

La protección de datos personales se encuentra reconocida en la Constitución peruana, reflejando la importancia de salvaguardar la información personal de los individuos en una sociedad digital en constante evolución, porque a medida que la tecnología avanza y la recopilación de datos se vuelve cada vez más omnipresente en la sociedad moderna, se requiere un mayor protagonismo a los mecanismos de protección que fiscalizan los datos personales y el impacto de esta protección constitucional se refleja en la promulgación de la Ley de Protección de Datos Personales (Ley Nº 29733) y su reglamento, que establecen directrices claras sobre cómo deben ser tratados los datos personales por parte de las entidades públicas y privadas, promoviendo la transparencia, la seguridad y la responsabilidad en el manejo de la información, como el legítimo tratamiento de datos para salvaguardar la integridad del titular de datos, por lo tanto, la relevancia constitucional de la protección de datos personales en el Perú es innegable y su impacto se extiende a todas las esferas de la sociedad.

4.2. Consecuencias jurídicas de la aplicación del principio de privacidad desde el diseño a innovaciones tecnológicas

En este apartado, se desarrolla como medida preventiva de las brechas de seguridad, la denominada “Privacidad desde el diseño” y como su origen permite practicas sólidas de privacidad, durante el tiempo de vida de los procesos que involucren tratamiento de datos personales, convirtiéndola en una propuesta innovadora que aborda desde un inicio la protección de datos personales, porque el funcionamiento de casi toda innovación tecnológica para un mejor desarrollo personalizado parte del tratamiento de datos personales, de las cuales, pueden ser tanto colectivas como individuales “Colectiva porque, por un lado, la información de un sujeto usualmente involucra datos de terceros (por ejemplo, el material genético). Por otro lado, las repercusiones de la pérdida de privacidad se experimentan comúnmente a nivel personal.” (Veliz, 2021, p. 433).

La PdD puede considerarse como una alternativa abstracta, por su propuesta de proteger los datos personales antes que se realicen las brechas de seguridad, sin embargo, se puede reconocer dentro de un estado de derecho generando consecuencias jurídicas, como es el caso de la Unión Europea, la cual, dentro del RGPD incorpora en el artículo 25, lineamientos obligatorios sobre los controladores de datos (las organizaciones que recopilan y procesan datos personales) implementando medidas técnicas y organizativas para garantizar que, por defecto, solo se procesen los datos necesarios para cada finalidad específica y que, por diseño, se proteja la

privacidad de los individuos.

También la AEPD, creó una guía de PdD, teniendo en cuenta, constantemente, compañías y entidades elaboran servicios que dependen en gran medida de la información personal, y dado que el efecto sobre la privacidad se amplifica gracias a la utilización de tecnologías innovadoras, resulta imprescindible implementar soluciones técnicas y organizativas efectivas y eficientes, en consecuencia, la guía tiene como propósito asegurar que se respeten los derechos y las libertades individuales en lo que concierne al manejo de datos personales.

La relevancia de la Guía de PdD, también recae por su incorporación de la "ingeniería de la privacidad", pues ha habido cuestionamientos sobre la efectividad de la PdD, porque "la definición actual de PbD no aborda el aspecto metodológico de la ingeniería de sistemas, es decir, no detalla los métodos de ingeniería de sistemas utilizados. Estos métodos deben cubrir todas las especificaciones técnicas del sistema y el ciclo de vida de los datos" (Palacios, D., Cousid, MP, y otros; p. 218; 2022). Sin embargo, la GPD, prevé este escenario, y póstula un proceso sistemático que tiene como objetivo traducir a los ingenieros de sistemas o encargados de software, concreta y funcionalmente los conceptos de PdD, en acciones implementables a lo largo de todo el ciclo de vida de los sistemas de información responsables de la gestión de datos personales.

En el marco legal y doctrinario europeo se aborda los posibles escenarios relacionados a la PdD y brinda una respuesta a ello, otorgando garantías legales y herramientas de aplicación de la PdD, como lo es la ingeniería de la privacidad. Paralelamente Julio Caisa en 2020, a través de su tesis doctoral "Contribución al Diseño de Sistemas Respetuosos con la Privacidad usando Patrones", aporta diseños de sistemas respetuosos a la privacidad, mediante la ingeniería de la privacidad al integrar la privacidad en el proceso de ingeniería de sistemas, brindando teorías, técnicas, métodos y herramientas de solución.

Se concluye que, como consecuencia jurídica de la incorporación del principio de PdD a innovaciones tecnológicas, es la modificación del RGPD en la Unión Europea, delimitando estándares de privacidad, porque menciona los sujetos obligados a la protección de datos desde el diseño y crea requisitos de evaluación de impacto de la privacidad antes de iniciar proyectos o actividades que involucren la recopilación y el procesamiento de datos personales, destinadas a garantizar que se respete la privacidad de las personas y se cumpla con las regulaciones de protección de datos en innovaciones tecnológicas, asimismo, las organizaciones deben ser conscientes de estas implicaciones legales y tomar medidas proactivas para cumplir con las leyes de privacidad y proteger los derechos de los individuos.

4.3. Criterios que permitan materializar la privacidad desde el diseño como principio jurídico en el ordenamiento peruano

Como último apartado, se sustentarán criterios que permitan materializar la PdD como principio jurídico en el ordenamiento peruano, partiendo por identificarlo dentro del contexto peruano, pues actuará como principio que guiaría la interpretación y aplicación de las normas jurídicas vinculada a la protección de los datos personales, tal como menciona en relación a la naturaleza de los principios, Atienza, M; & Ruiz,J (1991) " los principios jurídicos no admiten una enumeración taxativa, es decir, no se pueden encerrar en un listado definitivo. Esto no se debe únicamente a que los elementos que configuran sus requisitos de aplicación posean un margen de indeterminación más o menos amplio. La razón fundamental radica en que tales requisitos carecen, incluso, de una delimitación genérica precisa." (p.108).

Lo que se busca, es el cumplimiento del resguardo de los datos personales, no crear una regla concreta y especifica que solo actúen ante un supuesto de hecho determinado, sino que la PdD como principio sirva como patrón para la creación de leyes y marcos jurídicos orientados a la gestión de riesgos en la privacidad.

Es así, que la materialización de la PdD en Perú, incluye un enfoque metodológico entre la gestión de riesgos, centrado en la identificación y mitigación de amenazas a la privacidad, lo que es esencial para evaluar y minimizar los riesgos asociados con el tratamiento de datos y la Responsabilidad Proactiva, poniendo énfasis en la incorporación de medidas de privacidad desde el inicio de cualquier proyecto, producto o sistema que involucre datos personales.

Ambos enfoques no son mutuamente excluyentes; de hecho, son complementarios, pues al unirlos las organizaciones pueden fortalecer significativamente su postura en materia de privacidad y cumplimiento normativo, contribuyendo a construir una cultura de privacidad sólida y a mantener la confianza de los consumidores, al tiempo que ayuda a prevenir sanciones legales y problemas de reputación. Por lo tanto, estas estrategias son esenciales en un entorno donde la privacidad y la seguridad de datos son cada vez más importantes y reguladas.

Por tanto, la PdD se implementará como principio en la LPDP motivada en garantizar la protección del derecho fundamental de protección de datos personales desde una perspectiva preventiva, al no contar dentro del marco legal peruano con mecanismos proactivos, se sustentan, un desglosé no restrictivo de criterios clave que permite materializar la incorporación:

a.- Definición clara y precisa: "La privacidad desde el diseño, es un enfoque proactivo que configura la privacidad durante todo el ciclo de vida de productos, sistemas, servicios y

procesos que impliquen el tratamiento de datos personales".

b.-La Autoridad Nacional de Protección de datos será el órgano competente encargado de promover el nuevo principio en la administración privada y pública, como en los ciudadanos, además de fiscalizar y exigir su cumplimiento en las organizaciones que recopilan y procesan datos personales;

c.- Requerir de herramientas fundamentales para identificar y mitigar riesgos para la privacidad como las evaluaciones de impacto en la privacidad antes de iniciar proyectos que impliquen la recopilación y el procesamiento de datos personales;

d.- Certificaciones y Estándares de Privacidad: La ANPD podría promover la adopción de certificaciones y estándares de privacidad que permitan a las organizaciones demostrar su cumplimiento con el principio de PdD.

e.- Educación y Concienciación: La ANPD debe promover la educación y la concienciación sobre la importancia de la PdD, tanto entre las organizaciones como entre los ciudadanos para garantizar que se respeten los derechos y las preocupaciones de las personas.

La materialización de la PdD en la normativa peruana, requiere una definición clara, esto implica la integración obligatoria de medidas técnicas y organizativas por parte de las organizaciones o el titular del banco de datos encargado del tratamiento, con el fin de salvaguardar los datos personales en cada fase de planificación, desarrollo, implementación y gestión de sistemas que involucren su recopilación y procesamiento. Para cumplir con el principio de PdD, se requiere llevar a cabo evaluaciones de impacto en la privacidad y adoptar medidas de seguridad apropiadas, todo ello fundamentado en un enfoque dual de gestión de riesgos y responsabilidad proactiva.

4.4. Propuesta: Principio de Privacidad desde el Diseño en el Perú

Actualmente, el Perú no cuenta con blindaje preventivo de ciber ataques o brechas de seguridad, porque la legislación está regulada desde una perspectiva por defecto, dejando de cubrir todos los frentes de protección, en consecuencia se propone la incorporación del principio de la privacidad desde el diseño en la legislación peruana para ampliar la capacidad de protección y proporcionando garantías completas para el legítimo tratamiento de datos personales al enfocarse en la minimización de datos, la transparencia, la seguridad, la evaluación de impacto de privacidad y el cumplimiento normativo.

A continuación, se describen algunas de las garantías generadas por este principio:

a.- Minimización de Datos: La PdD promueve la recolección y el procesamiento de la cantidad mínima de datos necesarios para cumplir con el propósito específico. Esto garantiza que no se recopilen datos innecesarios o excesivos, lo que reduce el riesgo de exposición indebida de información personal;

b.- Transparencia y Consentimiento Informado: Las organizaciones que aplican la PdD deben informar a los individuos sobre cómo se utilizarán sus datos personales y obtener su consentimiento de manera informada. Esto garantiza que las personas estén plenamente conscientes de cómo se utilizarán sus datos y puedan ejercer un control significativo sobre su información;

c.- Seguridad Proactiva: La seguridad de los datos debe ser una característica inherente en todos los sistemas y procesos desde el inicio, materializados a través de la ingeniería de la privacidad. Esto garantiza que los datos estén protegidos de manera adecuada y que las vulnerabilidades de seguridad no se pasen por alto en ninguna etapa del tratamiento de datos;

d.- Evaluación de Impacto de Privacidad (EIPD): La realización de evaluaciones de impacto de privacidad en ciertos casos garantiza que los riesgos para los derechos y libertades de las personas sean identificados y mitigados de manera proactiva. Esta evaluación contribuye a un tratamiento de datos más seguro y garantiza la protección de los derechos de los individuos;

e.- Cumplimiento Normativo: La incorporación del principio de la PdD en la normativa peruana garantiza que las organizaciones cumplan con las regulaciones de privacidad. Esto proporciona una base sólida para la aplicación de sanciones en caso de incumplimiento, lo que a su vez actúa como un incentivo para el legítimo tratamiento de datos personales; y,

f.- Construcción de Confianza: Al demostrar un compromiso genuino con la protección de datos y la privacidad desde el inicio, las organizaciones pueden construir la confianza de sus clientes y usuarios. Esto es esencial en un entorno en el que la confianza en la gestión de datos es fundamental para la relación con los ciudadanos.

En un mundo digital en constante evolución, la incorporación del principio de la Privacidad desde el Diseño en la Ley N°29733 de Protección de Datos Personales representa un avance significativo que tiende a garantizar el legítimo tratamiento de datos personales en el país, al promover una cultura de privacidad proactiva, asegurando que la protección de datos será una consideración fundamental desde el inicio de cualquier proyecto o sistema tecnológico que involucre información personal.

Conclusiones

La relevancia constitucional del derecho fundamental de protección de datos personales es innegable, ya que salvaguarda la privacidad y la dignidad de los individuos en una sociedad digital en constante evolución. Este derecho, respaldado por la doctrina y jurisprudencia comparada, se traduce en la obligación de las organizaciones de garantizar la transparencia, la seguridad y el consentimiento informado en el tratamiento de datos, promoviendo la responsabilidad en el manejo de la información personal, lo que contribuye a preservar la integridad de los titulares de datos.

Las principales consecuencias jurídicas de la aplicación del principio de Privacidad desde el Diseño a innovaciones tecnológicas, tales como la transparencia, la seguridad y la responsabilidad en el tratamiento de datos, fortaleciendo la confianza de los usuarios en las innovaciones tecnológicas, las cuales, son cruciales para garantizar un equilibrio entre la innovación tecnológica y la protección de la privacidad de las personas.

Finalmente, la materialización de la Privacidad desde el Diseño en la normativa peruana será esencial para abordar los desafíos de la sociedad digital, al incorporar una medida proactiva, faltante en una legislación regulada únicamente por defecto, generando un entorno de confianza en el tratamiento de datos personales, reduciendo sanciones legales y mejorando el blindaje del derecho fundamental de protección de datos personales.

Recomendaciones

A fin de fortalecer el resguardo al derecho fundamental de protección de datos personales y promover la confianza en la gestión de la información en la sociedad digital, se recomienda incorporar la privacidad desde el diseño en la Ley N°°29733 mediante un Decreto Supremo del Ministerio de Justicia y Derechos Humano, quien creó la LPDP, su reglamento y la ANPD. Adicionalmente, con miras de garantizar el legítimo tratamiento de datos personales, se recomienda aplicar los criterios jurídicos postulados previamente que permiten la materialización de la privacidad desde el diseño en la normativa peruana

Referencias Bibliográficas

Agencia Española de Protección de Datos. (2019). *Guía de privacidad desde diseño.* https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf

Alemany, J. (2020). *Medidas de protección de la privacidad en ambientes sociales* [Tesis doctoral, Universidad Politécnica de Valencia].

Alshammari, M. (2019). *A principled approach for engineering privacy by design* [Tesis doctoral, Universidad de Oxford].

Alvarez, A. (2021). *Justificación de la investigación* [Proyecto de investigación, Universidad de Lima].

American Psychological Association. (2010). *Publication manual of the American Psychological Association.* Author.

Arias, F. (2016). *El proyecto de investigación. Introducción a la metodología científica* (6ª ed.). Episteme.

Atienza, M., & Ruiz, J. (2001). Sobre principios y reglas. *Cuadernos de Filosofía del Derecho, 10*, 101-120.

Autoridad Nacional de Protección de Datos Personales. (2013). *El derecho fundamental a la protección de datos personales.* Ministerio de Justicia y Derechos Humanos.

Bernal, C. (2016). *Metodología de la investigación. Administración, economía, humanidades y ciencias sociales* (3ª ed.). Pearson Educación.

Bestard, J. (2021). *La gestión de datos personales y el delegado de protección de datos en la sanidad pública, con atención especial a la Comunidad de Madrid* [Tesis doctoral, Universidad Autónoma de Madrid].

Calo, R. (2010). The boundaries of privacy harm. *Indiana Law Journal, 86*(3), 31.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. *Identity in the Information Society, 3*, 247–251. https://doi.org/10.1007/s12394-010-0062-y

Cavoukian, A. (2010). *The 7 foundational principles implementation and mapping of fair information practices.*

Congreso de la República del Perú. (2011). *Ley N° 29733 - Ley de Protección de Datos Personales*. Diario Oficial El Peruano. https://www.minjus.gob.pe/ley-de-proteccion-de-datos-personales/

Duncan, W. R. (1996). *A guide to the project management body of knowledge. Project risk management* (6ª ed.). PMI Standards Committee, Project Management Institute.

Foro Económico Mundial. (2020). *Reporte de riesgos mundial.* https://es.weforum.org/reports/the-global-risks-report-2020

Hidalgo, Y. (2020). *El paradigma del derecho global para la protección de datos personales en redes sociales* [Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo].

Ley N° 29733, Ley de protección de datos personales y reglamento. (2011, 3 de julio). https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733

Londoño, A. (2021). *Tratamiento de datos personales a través de web cookies: Análisis bajo la legislación colombiana de protección de datos personales* [Tesis de maestría, Universidad de los Andes].

Martínez, M. (2017). Nuevos perfiles del derecho al olvido en Europa y España. *Anuario de la Facultad de Derecho de la Universidad de Alcalá, X*, 231-266. https://doi.org/10.2307/j.ctvq4bzjd.10

Olivos, M. (2019). La protección de la privacidad como objeto de tutela en el ordenamiento jurídico peruano. *Revista IUS, 1*(1), 47-67. https://doi.org/10.35383/ius.v1i1.38

Ontiveros, E., Vizcaíno, D., & López, V. (2016). *Las ciudades del futuro: Inteligentes, digitales y sostenibles.* Telefónica Fundación.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (2016, 27 de abril). https://www.boe.es/doue/2016/119/L00001-00088.pdf

Remolina, N., & Alvarez, L. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada —accountability— en las transferencias internacionales de datos personales.* Facultad de Derecho, GECTI.

Resolución Directoral N° 2564-2022-JUS/DGTAIPD-DPDP (Lima). (2022, 1 de julio). https://cdn.www.gob.pe/uploads/document/file/3672700/RD%202564-2022.pdf.pdf?v=1663884528

Saenz, L. (2020). *El Habeas Data en la actualidad.* Tribunal Constitucional: Centro de Estudios Constitucionales. https://www.tc.gob.pe/wp-content/uploads/2020/12/El-Habeas-Data-en-la-actualidad-1-1.pdf

Salinas, K. (2019). *La incompatibilidad existente en las obligaciones del derecho de información del titular de los datos personales* [Tesis de segunda especialidad, Pontificia Universidad Católica del Perú].

Santos, S. (2019). Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos. *Revista Facultad de Derecho PUCP, 83*, 179-206. https://doi.org/10.18800/derechopucp.201902.006

Sikora, D. (2017). Factores de desarrollo de las ciudades inteligentes. *Revista Universitaria de Geografía, 26*(1), 135-152.

Solove, D. J. (2021). *Understanding Privacy* (2nd ed.). Harvard University Press.

United States v. U.S. District Court, 407 U.S. 297, 314 (1972) (Caso Keith).

Véliz, C. (2021). Más sobre privacidad. Respuesta a los comentarios sobre "Privacidad es poder". *Eunomía. Revista en Cultura de la Legalidad, 21*, 431-434.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

Zamudio, M. (2021). *El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. Límites y propuestas* [Tesis de maestría, Pontificia Universidad Católica del Perú].

Anexos

Matriz de Consistencia

<table>
<tr><td colspan="3">TESISTA : Palestina Sabina Vargas Toscanelli</td></tr>
<tr><td colspan="3">ASESORA: Katherinee del Pilar Alvarado Tapia</td></tr>
<tr><td colspan="3">LINEA DE INVETIGACION: DEMOCRACIA, GOBERNABILIDAD GESTIÓN PÚBLICA</td></tr>
<tr><td colspan="3">TITULO: Incorporación de la privacidad desde el diseño como principio fundamental que garantice el legítimo tratamiento de datos personales en Perú</td></tr>
<tr><td colspan="3">PROBLEMA: ¿Por qué se garantizará el tratamiento legítimo de datos personales mediante la incorporación del principio de privacidad desde el diseño en la normativa jurídica peruana?</td></tr>
<tr><td colspan="3">CATEGORIAS CONCEPTUALES</td></tr>
<tr><td colspan="2">DERECHO FUNDAMENTAL DE DATOS PERSONALES</td><td>PRIVACIDADAD DESDE EL DISEÑO</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">OBJETIVOS</td></tr>
<tr><td colspan="3">GENERAL: “GARANTIZAR EL LEGITIMO TRATAMIENTO DE DATOS PERSONALES MEDIANTE LA INCORPORACION DEL PRINCIPIO DE LA PRIVACIDAD DESDE EL DISEÑO EN LA NORMATIVA PERUANA”</td></tr>
<tr><td rowspan="3">ESPECIFICOS</td><td colspan="2">1. Analizar la relevancia constitucional de la tutela de derecho fundamental de protección de datos personales y evaluar su impacto en
el tratamiento de datos, a partir de la doctrina y jurisprudencia comparada</td></tr>
<tr><td colspan="2">2. Determinar las consecuencias jurídicas de la aplicación del principio de privacidad desde el diseño a innovaciones tecnológicas</td></tr>
<tr><td colspan="2">3. Sustentar criterios que permitan materializar la privacidad desde el diseño como principio jurídico en el ordenamiento peruano</td></tr>
<tr><td>HIPOTESIS</td><td colspan="2">SI SE INCORPORA LA PRIVACIDAD DESDE EL DISEÑO MEDIANTE UN
PRINCIPIO JURIDICO EN LA NORMATIVA PERUANA ENTONCES SE GARANTIZARÁ EL LEGITIMO TRATAMIENTO DE DATOS PERSONALES</td></tr>
<tr><td colspan="3">APORTE</td></tr>
<tr><td colspan="3">GARANTIZAR EL LEGITIMO TRATAMIENTO DE DATOS PERSONALES MEDIANTE LA INCORPORACION EN LA NORMATIVA PERUANA DEL PRINCIPIO DE LA PRIVACIDAD DESDE EL DISEÑO</td></tr>
</table>

Esquema de Resultados y Discusión

Objetivo Especifico	Esquema de Resultados
Analizar la relevancia constitucional de la tutela de derecho fundamental de protección de datos personales y evaluar su impacto en el tratamiento de datos, a partir de la doctrina y jurisprudencia comparada	3.1. Análisis de la relevancia constitucional de la tutela del derecho fundamental de protección de datos personales y evaluar su impacto en el tratamiento de datos 3.1.1. Reconocimiento constitucional de la protección de datos personales como derecho fundamental 3.1.2. Mecanismos de Protección para el legítimo tratamiento de datos personales mediante jurisprudencia comparada
Determinar las consecuencias jurídicas de la aplicación del principio de privacidad desde el diseño a innovaciones tecnológicas	3.2. Consecuencias jurídicas de la aplicación del principio de privacidad desde el diseño a innovaciones tecnológicas
Sustentar criterios que permitan materializar la privacidad desde el diseño como principio jurídico en el ordenamiento peruano	3.3. Criterios que permitan materializar la privacidad desde el diseño como principio jurídico en el ordenamiento peruano
Objetivo General: Garantizar el legítimo tratamiento de datos personales mediante la incorporación del principio de la privacidad desde el diseño en la normativa peruana	**PROPUESTA**