

**UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL
DE HUAMANGA**

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO



TESIS:

**El derecho a la protección de datos personales frente a
sistemas de vigilancia digital en el sector público peruano.**

Para optar el título profesional de:
ABOGADA

PRESENTADO POR:
Bach. Fayruz Ingrid HINOSTROZA CUADROS

ASESOR:
Mtro. Jesús Walter ESPINOZA ALTAMIRANO

AYACUCHO - PERÚ

2026

DEDICATORIA

Con amor infinito, dedico esta tesis a mi madre, Mariela, quien me ha enseñado que el esfuerzo constante es el camino hacia los grandes logros. Gracias por ser mi apoyo incondicional, mi inspiración diaria y la fuerza que me impulsa a seguir adelante. Este logro también es tuyo.

AGRADECIMIENTO

A la universidad y a mis docentes, por compartir sus conocimientos, orientarme en la formación académica y haber sembrado en mí el compromiso con la ética y el rigor científico.

ÍNDICE DE CONTENIDO

DEDICATORIA	ii
Agradecimiento	iii
ÍNDICE DE TABLAS	vi
RESUMEN	vii
ABSTRACT	viii
INTRODUCCIÓN	9
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA	11
1.1. Descripción de la situación problemática	11
1.2. Formulación del problema	13
1.2.1. Problema principal	13
1.2.2. Problemas secundarios	13
1.3. Objetivos de la investigación	13
1.3.1. Objetivo General	13
1.3.2. Objetivo Específico	13
1.4. Justificación e importancia	14
1.4.1. Importancia de la investigación	15
1.4.2. Viabilidad de la investigación	15
1.5. Limitaciones de estudio	16
1.6. Delimitación de la investigación	16
1.6.1. Delimitación temporal	16
1.6.2. Delimitación temática	16
1.6.3. Delimitación normativa	17
CAPÍTULO II: MARCO TEÓRICO	18
2.1. Antecedentes de la investigación	18
2.2. Bases teóricas	19
2.2.1. Derechos fundamentales y protección de la persona	19
2.2.2. Derecho a la privacidad y derecho a la intimidad	25
2.2.3. Derecho fundamental a la protección de datos personales	30

2.2.4.	Sistemas de vigilancia digital	38
2.2.5.	Tratamiento de datos personales en el sector público	43
2.2.6.	Gobierno digital y transformación digital del Estado	48
2.2.7.	Tutela jurídica del derecho a la protección de datos personales	51
2.3.	Marco normativo	55
2.3.1.	Constitución Política del Perú	55
2.3.2.	Ley N.º 29733 — Ley de Protección de Datos Personales	56
2.3.3.	Reglamento de la Ley de Protección de Datos Personales	57
2.3.4.	Normativa sobre gobierno digital	58
2.3.5.	Jurisprudencia del Tribunal Constitucional	58
2.4.	Marco conceptual	59
2.4.1.	Derecho fundamental	59
2.4.2.	Protección de datos personales	59
2.4.3.	Datos personales	60
2.4.4.	Vigilancia digital	60
2.4.5.	Intimidad	60
2.4.6.	Privacidad	60
2.4.7.	Autodeterminación informativa	60
2.4.8.	Sector público	61
2.4.9.	Tratamiento de datos personales	61
2.4.10.	Seguridad de la información	61
CAPÍTULO III:	CATEGORÍAS	62
3.1.	Categorías y subcategorías de análisis	62
3.2.	Cuadro de categorización	64
CAPÍTULO IV:	METODOLOGÍA DE LA INVESTIGACIÓN	66
4.1.	Enfoque de investigación	66
4.2.	Nivel de investigación	66
4.3.	Tipo de investigación	66
4.4.	Método de la Investigación	67
4.5.	Diseño de la investigación	67
4.6.	Población y Muestra	67
4.6.1.	Población	67
4.6.2.	Muestra	68

4.7. Técnicas en instrumentos de recojo de la información	68
4.7.1. Técnicas de recojo de información	68
4.7.2. Instrumentos de recojo de información	69
4.8. Aspectos éticos	69
CAPÍTULO V: presentación de resultados	70
5.1. Resultados de la ficha documental	70
5.2. Resultados de las entrevistas	78
capítulo vi: Discusión de resultados	85
6.1. Propuesta de incorporación normativa a la Ley N.º 29733	86
CONCLUSIONES	88
RECOMENDACIONES	90
BIBLIOGRAFÍA	91
ANEXOS	95

ÍNDICE DE TABLAS

<i>Tabla 1 Ficha de análisis documental N.º F-01</i>	70
<i>Tabla 2 Ficha de análisis documental N.º F-02</i>	72
<i>Tabla 3 Ficha de análisis documental N.º F-03</i>	74
<i>Tabla 4 Ficha de análisis documental N.º F-04</i>	75
<i>Tabla 5 Ficha de análisis documental N.º F-05</i>	76
<i>Tabla 6 Ficha de análisis documental N.º F-06</i>	77
<i>Tabla 7 Categoría 1: Protección del derecho fundamental a los datos personales</i>	78
<i>Tabla 8 Categoría 2: Sistemas de vigilancia digital en el sector público</i>	80
<i>Tabla 9 Categoría 3: Límites jurídicos del tratamiento de datos personales</i>	82
<i>Tabla 10 Categoría 4: Vacíos del marco normativo</i>	83

RESUMEN

La presente investigación analiza la protección del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano, en un contexto caracterizado por el avance acelerado de las tecnologías de la información. El objetivo principal fue determinar los límites jurídicos del tratamiento de datos personales, así como identificar los vacíos normativos existentes en la regulación de dichas tecnologías.

La investigación se desarrolló bajo un enfoque cualitativo, de tipo básico y nivel descriptivo-explicativo, empleando como técnicas el análisis documental y la entrevista a especialistas en la materia. Los resultados evidenciaron que, si bien el ordenamiento jurídico peruano reconoce formalmente el derecho a la protección de datos personales, su aplicación resulta insuficiente frente a los desafíos de la vigilancia digital. Asimismo, se identificaron vacíos normativos relacionados con la falta de regulación específica sobre tecnologías emergentes, deficiencias en la implementación por parte de las entidades públicas y una limitada eficacia de los mecanismos de control y supervisión.

En conclusión, se determinó que existe una brecha entre el reconocimiento formal del derecho y su protección efectiva en la práctica, lo que exige una reforma integral del marco normativo que incorpore estándares más rigurosos, mecanismos de control eficaces y regulación específica sobre sistemas de vigilancia digital. Finalmente, se propone la implementación de lineamientos normativos orientados a fortalecer la tutela del derecho a los datos personales en el contexto de la transformación digital del Estado.

Palabras clave: protección de datos personales, vigilancia digital, sector público, autodeterminación informativa, límites jurídicos.

ABSTRACT

This research analyzes the protection of the fundamental right to personal data in the context of digital surveillance systems used in the Peruvian public sector, within a scenario characterized by the rapid advancement of information technologies. The main objective was to determine the legal limits of personal data processing and to identify existing regulatory gaps in the governance of such technologies.

The study was conducted under a qualitative approach, with a basic and descriptive-explanatory level, using documentary analysis and expert interviews as data collection techniques. The findings revealed that, although the Peruvian legal system formally recognizes the right to personal data protection, its application is insufficient in addressing the challenges posed by digital surveillance. Additionally, regulatory gaps were identified, including the lack of specific rules for emerging technologies, deficiencies in implementation by public entities, and limited effectiveness of control and supervisory mechanisms.

In conclusion, a gap exists between the formal recognition of the right and its effective protection in practice, which calls for a comprehensive reform of the legal framework, incorporating stricter standards, effective oversight mechanisms, and specific regulation of digital surveillance systems. Finally, the study proposes normative guidelines aimed at strengthening the protection of personal data rights within the context of the State's digital transformation.

Keywords: personal data protection, digital surveillance, public sector, informational self-determination, legal limits.

INTRODUCCIÓN

En el contexto de la transformación digital del Estado, el uso de tecnologías de información y comunicación ha generado nuevas formas de gestión pública orientadas a la eficiencia, seguridad y control social. En este escenario, los sistemas de vigilancia digital —como cámaras inteligentes, reconocimiento facial y monitoreo automatizado— han sido progresivamente incorporados por las entidades públicas; sin embargo, su implementación plantea serios desafíos en relación con la protección del derecho fundamental a los datos personales.

En el ordenamiento jurídico peruano, dicho derecho se encuentra reconocido a nivel constitucional y desarrollado mediante la Ley N.º 29733 y su reglamento. No obstante, tal como se evidencia en la realidad problemática, existe un desfase entre la regulación vigente y el avance de las tecnologías digitales, lo que genera vacíos normativos, debilidades en los mecanismos de control y riesgos de vulneración de derechos fundamentales. En particular, la ausencia de regulación específica sobre sistemas de vigilancia digital en el sector público configura un escenario de inseguridad jurídica y limitada tutela efectiva del derecho a la autodeterminación informativa.

En ese sentido, la presente investigación tiene como objetivo analizar los límites jurídicos del tratamiento de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano, así como identificar los vacíos normativos existentes y proponer lineamientos que permitan fortalecer la protección de los derechos fundamentales en el contexto de la sociedad digital.

Metodológicamente, la investigación se enmarca en un enfoque cualitativo con alcance descriptivo-explicativo, empleando técnicas como el análisis documental y la entrevista a especialistas, lo que permitió obtener información relevante sobre la regulación vigente, su aplicación práctica y los desafíos actuales en materia de protección de datos personales.

En cuanto a su estructura, la tesis se encuentra organizada en los siguientes capítulos:

- **Capítulo I: Planteamiento del problema**, en el cual se desarrolla la realidad problemática, la formulación del problema, los objetivos de la investigación, la justificación, la delimitación y el enfoque metodológico.

- **Capítulo II: Marco teórico**, donde se abordan los fundamentos doctrinarios, normativos y jurisprudenciales relacionados con la protección de datos personales, la autodeterminación informativa, los sistemas de vigilancia digital y los límites jurídicos del tratamiento de datos.
- **Capítulo III: Metodología de la investigación**, que describe el tipo y diseño de investigación, población y muestra, técnicas e instrumentos de recolección de datos, así como los procedimientos de análisis.
- **Capítulo IV: Resultados y discusión**, en el que se presentan los hallazgos obtenidos a partir del análisis documental y las entrevistas, organizados en categorías, así como su respectiva interpretación y contraste con el marco teórico y los antecedentes.
- **Capítulo V: Conclusiones y recomendaciones**, donde se exponen los principales resultados de la investigación en relación con los objetivos planteados, así como propuestas concretas orientadas a mejorar la protección del derecho a los datos personales en el sector público.

Finalmente, la investigación incluye un apartado de **propuesta normativa**, en el cual se plantean lineamientos específicos para la regulación de los sistemas de vigilancia digital, con el propósito de contribuir al fortalecimiento del marco jurídico peruano frente a los desafíos de la transformación digital.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1.Descripción de la situación problemática

En el contexto contemporáneo, el avance acelerado de las tecnologías digitales ha generado nuevos desafíos para la protección de los derechos fundamentales, particularmente el derecho a la protección de los datos personales frente al uso de sistemas de vigilancia digital por parte del Estado. El proceso de transformación digital de la administración pública peruana ha incrementado el uso de herramientas tecnológicas como cámaras de videovigilancia, sistemas biométricos, bases de datos estatales y mecanismos de monitoreo electrónico, lo cual plantea importantes tensiones entre la seguridad pública y la protección de la privacidad de los ciudadanos.

En el ordenamiento jurídico peruano, el derecho a la protección de los datos personales tiene reconocimiento constitucional en el artículo 2, inciso 6, de la Constitución Política del Perú, que establece que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte su intimidad personal o familiar (Zamudio Salinas, 2022). Este reconocimiento responde a la necesidad de proteger la dignidad humana y la autodeterminación informativa en un contexto de creciente digitalización de la información personal.

Asimismo, el desarrollo legislativo de este derecho se concretó con la promulgación de la Ley N.º 29733, Ley de Protección de Datos Personales, cuyo objeto es garantizar el derecho fundamental a la protección de los datos personales mediante su adecuado tratamiento y regulación por parte de entidades públicas y privadas (Congreso de la República del Perú, 2011). Esta normativa establece principios como legalidad, consentimiento, finalidad, proporcionalidad y seguridad en el tratamiento de datos personales, prohibiendo su recopilación mediante medios ilícitos o desleales (Olivos, 2020).

No obstante, pese a la existencia de este marco normativo, el avance de las tecnologías digitales ha generado nuevos escenarios de riesgo vinculados al uso masivo de información personal por parte de entidades públicas. La implementación de políticas de gobierno digital y sistemas tecnológicos en la administración pública ha incrementado el tratamiento de datos personales, generando desafíos relacionados con la protección de

la intimidad y la autodeterminación informativa de los ciudadanos (Salinas, 2022; Roel Alva et al., 2024).

En efecto, el desarrollo de tecnologías como la inteligencia artificial, los sistemas biométricos y los mecanismos de vigilancia digital permite la recopilación, almacenamiento y procesamiento masivo de información personal, lo que puede generar afectaciones a derechos fundamentales cuando no existen mecanismos adecuados de control, supervisión y transparencia (Roel Alva et al., 2024). En este sentido, la autodeterminación informativa faculta al individuo a controlar la información que le concierne, constituyendo un elemento esencial del Estado constitucional de derecho.

De igual manera, la expansión del entorno digital ha evidenciado vacíos regulatorios en la legislación peruana respecto a la gestión de datos personales en plataformas digitales y sistemas tecnológicos complejos. Aunque la Ley N.º 29733 establece principios generales de protección, existen limitaciones en su aplicación frente a nuevas formas de tratamiento de datos, como el uso de información en entornos digitales y sistemas de vigilancia masiva (Vargas Delgado, 2023; Guzmán Velarde, 2020).

En el ámbito del sector público, esta problemática adquiere mayor relevancia debido al poder que posee el Estado para recopilar y gestionar grandes volúmenes de información personal. El uso de sistemas de vigilancia digital puede generar riesgos de tratamiento indebido de datos personales, afectación a la privacidad, vigilancia excesiva y posibles vulneraciones a derechos fundamentales si no se establecen límites claros y mecanismos de control eficaces.

Asimismo, el proceso de modernización del Estado peruano mediante políticas de gobierno digital ha incrementado el uso de bases de datos interconectadas, sistemas de identificación y mecanismos de control electrónico, lo que exige el fortalecimiento del marco normativo y de las garantías jurídicas para evitar abusos en el tratamiento de datos personales y asegurar el respeto de los derechos fundamentales (Congreso de la República del Perú, 2011).

En consecuencia, se evidencia la existencia de una problemática jurídica vinculada a la insuficiente regulación y control del uso de sistemas de vigilancia digital en el sector público peruano, lo cual genera tensiones entre la seguridad pública, la eficiencia administrativa y la protección del derecho fundamental a los datos personales.

Esta situación justifica la necesidad de realizar un análisis jurídico-dogmático sobre la tutela del derecho a la protección de datos personales frente a los sistemas de vigilancia digital en el Perú.

1.2. Formulación del problema

1.2.1. Problema principal

¿De qué manera se encuentra jurídicamente protegida la tutela del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano?

1.2.2. Problemas secundarios

a. Primer problema secundario

¿Cuáles son los límites jurídicos del tratamiento de datos personales por parte de las entidades del sector público mediante sistemas de vigilancia digital en el Perú?

b. Segundo problema secundario

¿Qué vacíos o limitaciones presenta el marco normativo peruano en la protección del derecho a los datos personales frente al uso de sistemas de vigilancia digital en la administración pública?

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Analizar la protección jurídica del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano.

1.3.2. Objetivo Específico

a. Primer objetivo Especifico

Determinar los límites jurídicos del tratamiento de datos personales por parte de las entidades del sector público mediante sistemas de vigilancia digital en el Perú.

b. Segundo objetivo Especifico

Identificar los vacíos o limitaciones del marco normativo peruano en la protección del derecho a los datos personales frente al uso de sistemas de vigilancia digital en la administración pública.

1.4. Justificación e importancia

a. Justificación teórica

La presente investigación se justifica en el ámbito teórico debido a que contribuye al desarrollo del conocimiento jurídico sobre la protección del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. En el contexto actual de transformación digital del Estado, el tratamiento masivo de datos personales por parte de entidades públicas plantea nuevos desafíos para la tutela de los derechos fundamentales, particularmente en relación con la privacidad, la autodeterminación informativa y la dignidad de la persona.

El estudio permite fortalecer el análisis doctrinario y jurídico del derecho a la protección de datos personales en el ordenamiento constitucional peruano, así como examinar los límites del poder estatal en el tratamiento de información personal mediante tecnologías de vigilancia digital. Asimismo, la investigación aporta elementos conceptuales y doctrinarios que permiten comprender la relación entre el avance tecnológico y la protección de los derechos fundamentales en el Estado constitucional de derecho.

b. Justificación práctica

La investigación posee relevancia práctica debido a que el análisis del marco normativo sobre protección de datos personales frente a sistemas de vigilancia digital permite identificar vacíos, limitaciones o deficiencias en la regulación vigente aplicable al sector público peruano.

Los resultados del estudio pueden contribuir al fortalecimiento de las garantías jurídicas en el tratamiento de datos personales por parte de las entidades estatales, promoviendo el respeto de los derechos fundamentales de los ciudadanos frente al uso de tecnologías de vigilancia digital. Asimismo, la investigación puede servir como referencia para la formulación de políticas públicas, reformas normativas y mecanismos de control

que aseguren un adecuado equilibrio entre la seguridad pública, la eficiencia administrativa y la protección de la privacidad.

c. Justificación social

Desde el punto de vista social, la investigación resulta relevante debido a que la protección de los datos personales constituye una garantía esencial para la defensa de la dignidad humana, la libertad individual y la protección de la intimidad en la sociedad digital. El uso creciente de tecnologías de vigilancia por parte del Estado puede generar riesgos de afectación a los derechos fundamentales si no existen mecanismos adecuados de regulación y control.

En este sentido, el estudio busca contribuir al fortalecimiento de la protección de los derechos fundamentales de los ciudadanos frente al tratamiento indebido de información personal, promoviendo el respeto de la privacidad y la transparencia en la actuación de la administración pública.

1.4.1.Importancia de la investigación

La importancia del estudio radica en que aborda una problemática jurídica actual vinculada al impacto del desarrollo tecnológico en la protección de los derechos fundamentales dentro del Estado peruano. La investigación busca aportar fundamentos jurídicos que permitan fortalecer la tutela del derecho a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público, contribuyendo al desarrollo del derecho constitucional y al fortalecimiento del Estado de derecho.

Asimismo, la investigación resulta relevante para el ámbito académico, jurídico e institucional, al generar aportes doctrinarios y normativos que promuevan el respeto de los derechos fundamentales en el contexto de la transformación digital de la administración pública.

1.4.2.Viabilidad de la investigación

La presente investigación resultó viable debido a la disponibilidad de fuentes normativas, doctrinarias y jurisprudenciales necesarias para el análisis jurídico del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano.

Existe acceso a normativa vigente relevante, como la Constitución Política del Perú, la Ley N.º 29733, Ley de Protección de Datos Personales, su reglamento aprobado mediante Decreto Supremo N.º 003-2013-JUS, así como normativa complementaria sobre gobierno digital y administración pública. Asimismo, se cuenta con jurisprudencia del Tribunal Constitucional y pronunciamientos de la Autoridad Nacional de Protección de Datos Personales, lo cual permite realizar un análisis jurídico-dogmático del objeto de estudio.

1.5.Limitaciones de estudio

La presente investigación presenta ciertas limitaciones propias de su naturaleza jurídico-dogmática y documental. En primer lugar, el estudio se circunscribe al análisis del marco normativo, doctrinario y jurisprudencial peruano relacionado con la protección de datos personales y el uso de sistemas de vigilancia digital en el sector público, por lo que no incorpora evidencia empírica ni estudios de campo sobre la aplicación práctica de dichas normas en entidades estatales. Asimismo, la rápida evolución de las tecnologías de vigilancia digital constituye una limitación, debido a que el desarrollo tecnológico suele avanzar con mayor rapidez que la producción normativa, generando escenarios cambiantes y nuevos desafíos jurídicos.

1.6.Delimitación de la investigación

1.6.1.Delimitación temporal

El estudio comprende el periodo 2020–2025, considerando que en este intervalo se ha intensificado el proceso de transformación digital del Estado peruano, el uso de tecnologías de vigilancia digital y la implementación de políticas de gobierno digital, lo cual permite analizar la problemática en su contexto actual.

1.6.2.Delimitación temática

La investigación se enfoca en el análisis del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público, comprendiendo aspectos vinculados a la autodeterminación informativa, la privacidad, el tratamiento de datos personales y los límites jurídicos del uso de tecnologías de vigilancia por parte del Estado.

No constituye objeto de estudio el tratamiento de datos personales en el sector privado ni los aspectos técnicos o informáticos del funcionamiento de los sistemas de vigilancia digital, sino únicamente su dimensión jurídica y constitucional.

1.6.3.Delimitación normativa

El estudio se desarrolla dentro del marco de la normativa peruana vigente sobre protección de datos personales, principalmente:

- Constitución Política del Perú (artículo 2 inciso 6).
- Ley N.º 29733, Ley de Protección de Datos Personales.
- Reglamento de la Ley de Protección de Datos Personales (D.S. N.º 003-2013-JUS).
- Normativa sobre gobierno digital y administración pública.
- Jurisprudencia del Tribunal Constitucional relacionada con el derecho a la intimidad y protección de datos personales.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

Haro Benites y Moncada Hernández (2024) desarrollaron la tesis titulada “Constitucionalidad de la vigilancia masiva en el tratamiento de los datos personales en relación al derecho a la intimidad”, en la Universidad de Piura, cuyo objetivo fue analizar la constitucionalidad del uso de mecanismos de vigilancia masiva y su relación con el derecho a la intimidad y la protección de datos personales. La investigación concluyó que la vigilancia masiva puede generar afectaciones a derechos fundamentales si no se establecen límites jurídicos claros, controles adecuados y garantías constitucionales en el tratamiento de la información personal. Este estudio aporta al presente trabajo al evidenciar los riesgos del uso de sistemas de vigilancia estatal sobre los derechos fundamentales.

Córdova Abregú (2023), en su investigación “Tratamiento de datos personales en el marco de la atención de las solicitudes de acceso a la información pública” desarrollada en la Pontificia Universidad Católica del Perú, analizó la relación entre el derecho de acceso a la información pública y el derecho a la protección de datos personales. El estudio determinó que existe tensión entre ambos derechos fundamentales, lo que exige mecanismos de equilibrio para evitar vulneraciones a la privacidad en la actuación estatal. Este antecedente contribuye al presente estudio al evidenciar la necesidad de límites en el tratamiento de datos por entidades públicas.

Acevedo Paredes y Paredes Torres (2024) realizaron la tesis titulada “El efecto que causa la inteligencia artificial en la protección de datos personales bajo la Ley N.º 29733, Perú”, cuyo objetivo fue analizar el impacto de la inteligencia artificial en la protección de datos personales en el marco normativo peruano. La investigación concluyó que el avance tecnológico genera nuevos desafíos regulatorios y evidencia la necesidad de fortalecer los mecanismos de protección jurídica frente al tratamiento automatizado de datos personales. Este estudio aporta al presente trabajo al demostrar la relación entre tecnologías digitales y protección de derechos fundamentales.

Mejía Arbildo (2023) desarrolló la tesis “Inteligencia artificial y sus efectos en la protección de datos personales en la Ley N.º 29733, Lima 2023”, cuyo propósito fue analizar los efectos del uso de tecnologías digitales en la protección de datos personales.

El estudio empleó un enfoque cualitativo y concluyó que el marco normativo peruano presenta limitaciones frente al tratamiento masivo de datos mediante sistemas tecnológicos, lo que evidencia la necesidad de fortalecer la regulación jurídica. Este antecedente contribuye al presente estudio al identificar vacíos normativos en la protección de datos personales.

Chorres Céspedes (2024) desarrolló la investigación “Impacto de la tecnología en la protección de datos personales desde el derecho constitucional”, cuyo objetivo fue analizar el impacto del entorno digital en la protección jurídica de los datos personales. El estudio concluyó que el desarrollo tecnológico exige la actualización del marco jurídico para garantizar la protección efectiva de los derechos fundamentales en el entorno digital. Este antecedente aporta al presente estudio al evidenciar la necesidad de fortalecer la tutela constitucional frente al avance tecnológico.

2.2.Bases teóricas

2.2.1.Derechos fundamentales y protección de la persona

El derecho fundamental a la protección de datos personales constituye una manifestación moderna de los derechos fundamentales vinculados a la dignidad humana, la libertad individual y la protección de la vida privada en el contexto de la sociedad de la información. Este derecho se orienta a garantizar que toda persona tenga control sobre la información que le concierne, evitando el tratamiento arbitrario o indebido de sus datos personales. Según Pérez Luño (2016), el desarrollo de las tecnologías de la información ha generado nuevas formas de vulneración de los derechos fundamentales, lo que ha hecho necesaria la creación de mecanismos jurídicos que protejan la información personal frente al uso indiscriminado de herramientas tecnológicas. En este sentido, el derecho a la protección de datos personales surge como respuesta a los riesgos derivados del procesamiento automatizado de información en las sociedades contemporáneas.

Desde una perspectiva conceptual, el derecho a la protección de datos personales se vincula estrechamente con el principio de autodeterminación informativa, entendido como la facultad que posee toda persona para decidir sobre la recopilación, uso y difusión de sus datos personales. Este concepto fue desarrollado inicialmente por el Tribunal Constitucional Federal alemán y posteriormente incorporado en diversos ordenamientos jurídicos como garantía esencial de la libertad individual (Alexy, 2007). La

autodeterminación informativa reconoce el poder del individuo para controlar su información personal y evitar su utilización sin consentimiento, constituyéndose en un elemento fundamental del Estado constitucional de derecho y en una garantía frente al poder estatal y al desarrollo tecnológico.

En el ordenamiento jurídico peruano, el derecho a la protección de datos personales tiene reconocimiento constitucional en el artículo 2, inciso 6, de la Constitución Política del Perú, el cual establece el derecho de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte su intimidad personal y familiar. Este reconocimiento implica el deber del Estado de garantizar la protección de la información personal y regular su tratamiento conforme a principios como legalidad, consentimiento, proporcionalidad y finalidad (Eguiguren Praeli, 2019). Asimismo, la Ley N.º 29733, Ley de Protección de Datos Personales, desarrolla este derecho fundamental estableciendo reglas para el tratamiento de datos personales y mecanismos de tutela frente a su uso indebido.

Desde el punto de vista doctrinario, el derecho a la protección de datos personales se configura como un derecho autónomo que trasciende el tradicional derecho a la intimidad, pues no solo protege la esfera privada del individuo, sino también su identidad personal y su libertad frente al tratamiento de información (Troncoso Reigada, 2010). En ese sentido, este derecho no se limita a impedir intromisiones ilegítimas en la vida privada, sino que otorga al titular facultades de acceso, rectificación, cancelación y oposición respecto del tratamiento de sus datos personales, fortaleciendo así el control del individuo sobre su información en entornos digitales.

Finalmente, en el contexto actual de transformación digital y uso masivo de tecnologías por parte del Estado, la protección de datos personales adquiere especial relevancia como garantía de los derechos fundamentales frente al tratamiento automatizado de información. Como señala Ferrajoli (2011), los derechos fundamentales constituyen límites al ejercicio del poder estatal y mecanismos de protección de la persona frente a posibles abusos de autoridad. En este sentido, el derecho a la protección de datos personales cumple una función esencial en la protección de la dignidad humana y la preservación de las libertades individuales en la sociedad digital.

2.2.1.1. Concepto de derechos fundamentales

Los derechos fundamentales constituyen el conjunto de prerrogativas inherentes a la persona humana que gozan de reconocimiento y protección constitucional, orientadas a garantizar la dignidad, la libertad y la igualdad de los individuos dentro del Estado constitucional de derecho. Estos derechos representan límites al ejercicio del poder estatal y aseguran el respeto de las condiciones esenciales para el desarrollo integral de la persona. Según Ferrajoli (2011), los derechos fundamentales son derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto personas, ciudadanos o sujetos capaces de obrar, y cuya garantía constituye un elemento esencial del constitucionalismo contemporáneo.

Desde una perspectiva doctrinaria, los derechos fundamentales se configuran como principios jurídicos que establecen mandatos de optimización dirigidos a los poderes públicos, los cuales deben ser realizados en la mayor medida posible dentro de las posibilidades jurídicas y fácticas existentes. En este sentido, Alexy (2007) sostiene que los derechos fundamentales poseen una doble dimensión: por un lado, constituyen derechos subjetivos de los individuos frente al Estado, y por otro, representan principios objetivos que orientan todo el ordenamiento jurídico. Esta concepción resalta la función normativa de los derechos fundamentales como parámetros de validez y legitimidad de las actuaciones estatales.

Asimismo, los derechos fundamentales se encuentran estrechamente vinculados con el principio de dignidad humana, considerado el fundamento axiológico del sistema jurídico constitucional. La dignidad de la persona implica el reconocimiento de su valor intrínseco y la necesidad de garantizar condiciones que permitan el libre desarrollo de su personalidad. En este sentido, Pérez Luño (2016) señala que los derechos fundamentales constituyen instrumentos jurídicos destinados a proteger la dignidad humana frente a cualquier forma de arbitrariedad o abuso del poder, especialmente en contextos de transformación social y tecnológica.

En el ordenamiento jurídico peruano, los derechos fundamentales se encuentran reconocidos en la Constitución Política del Perú de 1993, particularmente en su artículo 2, el cual establece un catálogo de derechos esenciales que garantizan la libertad, la igualdad, la integridad y la protección de la persona. El Tribunal Constitucional peruano

ha señalado que los derechos fundamentales constituyen el núcleo esencial del Estado constitucional y representan límites al ejercicio del poder público, así como garantías para la protección de la persona humana (Eguiguren Praeli, 2019).

En consecuencia, los derechos fundamentales cumplen una función esencial en el sistema jurídico al garantizar la protección de la persona frente al poder estatal, orientar la actuación de los órganos públicos y asegurar el respeto de los valores constitucionales. Su reconocimiento y protección efectiva constituyen elementos indispensables para la vigencia del Estado de derecho y la tutela de las libertades individuales en las sociedades contemporáneas.

2.2.1.2. Características de los derechos fundamentales

Los derechos fundamentales se caracterizan por su universalidad, en tanto corresponden a todas las personas por su sola condición humana, sin distinción de ninguna naturaleza. Esta característica implica que su titularidad no depende de factores como nacionalidad, condición social o cualquier otra circunstancia, sino que deriva del reconocimiento de la dignidad humana como fundamento del ordenamiento jurídico. En este sentido, Ferrajoli (2011) sostiene que los derechos fundamentales son universales porque pertenecen a todos los individuos en cuanto personas y constituyen garantías frente al poder estatal.

Otra característica esencial de los derechos fundamentales es su carácter inalienable e irrenunciable, lo que significa que no pueden ser objeto de disposición, transferencia o renuncia por parte de sus titulares. Esta cualidad responde a su vinculación directa con la dignidad humana y el libre desarrollo de la persona. Según Pérez Luño (2016), los derechos fundamentales no pueden ser suprimidos ni limitados arbitrariamente, pues constituyen garantías esenciales para la protección de la libertad individual y la convivencia democrática.

Asimismo, los derechos fundamentales poseen carácter imprescriptible e inviolable, lo que implica que su ejercicio no se extingue por el transcurso del tiempo y que el Estado tiene la obligación de respetarlos y garantizarlos permanentemente. Alexy (2007) explica que los derechos fundamentales actúan como principios jurídicos que imponen mandatos de optimización, los cuales deben ser realizados en la mayor medida

posible dentro de las posibilidades jurídicas y fácticas existentes, constituyendo parámetros de validez para la actuación de los poderes públicos.

Finalmente, los derechos fundamentales presentan una doble dimensión subjetiva y objetiva. En su dimensión subjetiva, se configuran como derechos individuales exigibles frente al Estado, mientras que en su dimensión objetiva constituyen principios estructurales del ordenamiento jurídico que orientan la actuación de los poderes públicos y garantizan la vigencia del Estado constitucional de derecho (Eguiguren Praeli, 2019). Esta doble dimensión evidencia la relevancia de los derechos fundamentales como elementos esenciales del sistema jurídico contemporáneo.

2.2.1.3. Protección constitucional de los derechos fundamentales

La protección constitucional de los derechos fundamentales constituye uno de los pilares del Estado constitucional de derecho, en tanto garantiza la vigencia efectiva de las libertades individuales y limita el ejercicio del poder estatal. La Constitución se configura como norma suprema del ordenamiento jurídico, estableciendo el reconocimiento y la tutela de los derechos fundamentales como principios esenciales del sistema democrático. Según García Toma (2013), la protección constitucional implica el establecimiento de mecanismos jurídicos que aseguren el respeto, garantía y defensa de los derechos fundamentales frente a posibles vulneraciones.

En el ordenamiento jurídico peruano, la Constitución Política de 1993 reconoce un amplio catálogo de derechos fundamentales en su artículo 2, los cuales comprenden derechos civiles, políticos, económicos y sociales orientados a la protección integral de la persona humana. Este reconocimiento implica la obligación del Estado de respetar, proteger y promover dichos derechos, garantizando su ejercicio efectivo y estableciendo límites al poder público. En este sentido, el Tribunal Constitucional ha señalado que los derechos fundamentales constituyen el núcleo esencial del orden constitucional y fundamento de todo el sistema jurídico (Eguiguren Praeli, 2019).

Asimismo, la protección constitucional de los derechos fundamentales se materializa a través de mecanismos jurisdiccionales de tutela, tales como los procesos constitucionales destinados a restablecer el ejercicio de derechos vulnerados. En el caso peruano, el Código Procesal Constitucional regula mecanismos como el proceso de amparo, hábeas corpus, hábeas data y acción de cumplimiento, los cuales permiten

garantizar la eficacia de los derechos fundamentales frente a actos u omisiones de autoridades públicas o particulares (Landa Arroyo, 2017).

Finalmente, la protección constitucional de los derechos fundamentales también comprende el control de constitucionalidad de las normas y actos del poder público, el cual permite asegurar la supremacía de la Constitución y la vigencia de los derechos fundamentales. Este control puede ser ejercido por los órganos jurisdiccionales mediante la interpretación constitucional y la revisión de normas contrarias a la Constitución, garantizando así la protección efectiva de la dignidad humana y el respeto del Estado de derecho.

2.2.1.4.Límites al ejercicio de los derechos fundamentales

Los derechos fundamentales no tienen carácter absoluto, pues su ejercicio puede estar sujeto a determinados límites orientados a garantizar la convivencia social, el orden público y la protección de otros derechos fundamentales. En el Estado constitucional de derecho, los derechos fundamentales deben ejercerse en armonía con los derechos de los demás y con los intereses generales de la sociedad. Según Alexy (2007), los derechos fundamentales se configuran como principios jurídicos que establecen mandatos de optimización, lo que implica que su realización depende de las posibilidades jurídicas y fácticas existentes, pudiendo ser objeto de limitaciones cuando entran en conflicto con otros derechos o bienes constitucionalmente protegidos.

Desde una perspectiva doctrinaria, los límites al ejercicio de los derechos fundamentales se fundamentan en la necesidad de preservar el equilibrio entre la libertad individual y el interés público. En este sentido, Ferrajoli (2011) sostiene que el ejercicio de los derechos fundamentales se encuentra condicionado por la existencia de normas jurídicas que regulan su alcance y establecen restricciones legítimas orientadas a evitar abusos o afectaciones a terceros. Sin embargo, dichas limitaciones deben estar debidamente justificadas, ser razonables y respetar el contenido esencial del derecho, evitando cualquier forma de arbitrariedad por parte del Estado.

Asimismo, el principio de proporcionalidad constituye un criterio fundamental para evaluar la legitimidad de las restricciones a los derechos fundamentales. Este principio exige que toda limitación cumpla con los requisitos de idoneidad, necesidad y proporcionalidad en sentido estricto, garantizando que la restricción sea adecuada para

alcanzar un fin constitucional legítimo, que no exista una medida menos lesiva y que el beneficio obtenido justifique la limitación del derecho (Bernal Pulido, 2007). De esta manera, el principio de proporcionalidad actúa como un mecanismo de control frente a posibles excesos en el ejercicio del poder estatal.

En el ordenamiento jurídico peruano, la Constitución Política reconoce el ejercicio de los derechos fundamentales dentro del marco del respeto al orden público, la moral y la seguridad, estableciendo que su ejercicio no debe afectar los derechos de los demás ni el bienestar general. El Tribunal Constitucional peruano ha señalado que los derechos fundamentales pueden ser objeto de restricciones siempre que estas se encuentren previstas por la ley, respondan a fines constitucionalmente legítimos y respeten el contenido esencial del derecho (Eguiguren Praeli, 2019).

Finalmente, los límites al ejercicio de los derechos fundamentales constituyen mecanismos necesarios para garantizar la convivencia democrática y la vigencia del Estado de derecho. No obstante, dichas restricciones deben aplicarse de manera excepcional y bajo criterios de razonabilidad y proporcionalidad, a fin de evitar que el poder estatal vulnere la dignidad humana y las libertades individuales. En este sentido, la regulación de los límites a los derechos fundamentales cumple una función esencial en la protección del equilibrio entre libertad y autoridad en las sociedades contemporáneas.

2.2.2.Derecho a la privacidad y derecho a la intimidad

El derecho a la privacidad y el derecho a la intimidad constituyen manifestaciones esenciales de la protección de la persona humana frente a injerencias arbitrarias en su esfera personal. Ambos derechos tienen como finalidad garantizar un ámbito de autonomía individual libre de interferencias externas, permitiendo el libre desarrollo de la personalidad y la protección de la dignidad humana. Según Pérez Luño (2016), la privacidad representa un espacio reservado de la vida personal que debe permanecer protegido frente a intromisiones del Estado o de terceros, especialmente en contextos de avance tecnológico y tratamiento masivo de información.

Desde el punto de vista doctrinario, el derecho a la intimidad se refiere específicamente al ámbito más reservado de la vida personal y familiar del individuo, mientras que el derecho a la privacidad posee un alcance más amplio, comprendiendo el control sobre la información personal, la vida privada y las relaciones sociales del

individuo. En este sentido, Troncoso Reigada (2010) sostiene que la intimidad protege la esfera interna de la persona, mientras que la privacidad comprende el control de la información personal en distintos ámbitos de interacción social.

En el ordenamiento jurídico peruano, el derecho a la intimidad personal y familiar se encuentra reconocido en el artículo 2, inciso 7, de la Constitución Política del Perú, que garantiza el respeto de la vida privada y la protección frente a intromisiones arbitrarias. Asimismo, el Tribunal Constitucional ha señalado que el derecho a la intimidad protege la esfera personal del individuo frente a cualquier forma de injerencia indebida, constituyendo una garantía fundamental para la protección de la dignidad humana y la libertad individual (Eguiguren Praeli, 2019).

En la sociedad digital contemporánea, el derecho a la privacidad y el derecho a la intimidad han adquirido especial relevancia debido al uso de tecnologías de información, sistemas de vigilancia y tratamiento masivo de datos personales. El desarrollo tecnológico ha ampliado las posibilidades de acceso y difusión de información personal, generando nuevos desafíos para la protección de estos derechos fundamentales y evidenciando la necesidad de mecanismos jurídicos eficaces que garanticen su tutela frente al uso indebido de la información personal.

2.2.2.1. Concepto de privacidad

La privacidad es un derecho fundamental que protege el ámbito personal del individuo frente a intromisiones indebidas del Estado o de terceros, garantizando un espacio de autonomía en el cual la persona puede desarrollar libremente su vida personal, familiar y social. Este derecho se fundamenta en la dignidad humana y en el principio de libertad individual, permitiendo al individuo controlar la información relacionada con su vida privada. Según Westin (1967), la privacidad puede definirse como el derecho de las personas a determinar por sí mismas cuándo, cómo y en qué medida la información sobre ellas es comunicada a otros.

Desde una perspectiva jurídica, la privacidad implica la protección de la vida privada, las comunicaciones personales, la información individual y las relaciones interpersonales frente a injerencias arbitrarias. En este sentido, Pérez Luño (2016) señala que la privacidad constituye un derecho esencial en las sociedades democráticas, pues

garantiza la autonomía personal y limita el ejercicio del poder estatal, especialmente en contextos de desarrollo tecnológico y expansión de sistemas de información.

Asimismo, el concepto de privacidad ha evolucionado con el avance de las tecnologías digitales, ampliándose desde la protección del ámbito físico de la persona hacia la protección de la información personal en entornos digitales. El desarrollo de bases de datos, redes informáticas y sistemas de vigilancia ha generado nuevos riesgos para la privacidad, lo que ha motivado el reconocimiento del derecho a la protección de datos personales como una manifestación específica del derecho a la privacidad (Troncoso Reigada, 2010).

En el ordenamiento jurídico peruano, la privacidad se encuentra vinculada al derecho a la intimidad personal y familiar reconocido constitucionalmente, así como al derecho a la protección de datos personales. La protección de la privacidad implica el deber del Estado de garantizar mecanismos jurídicos que impidan el acceso, uso o difusión indebida de información personal, asegurando el respeto de la dignidad humana y el libre desarrollo de la personalidad en el marco del Estado constitucional de derecho.

2.2.2.2.Derecho a la intimidad personal y familiar

El derecho a la intimidad personal y familiar constituye un derecho fundamental que protege el ámbito más reservado de la vida del individuo frente a injerencias arbitrarias del Estado o de terceros. Este derecho garantiza un espacio de autonomía personal en el cual la persona puede desarrollar su vida privada sin interferencias externas, preservando su dignidad, libertad y desarrollo integral. Según Pérez Luño (2016), el derecho a la intimidad protege el núcleo esencial de la vida privada del individuo, asegurando la existencia de un ámbito personal inaccesible a terceros sin el consentimiento del titular.

Desde una perspectiva doctrinaria, el derecho a la intimidad comprende la protección de aspectos relacionados con la vida personal, familiar, comunicaciones, convicciones, información personal y relaciones interpersonales. En este sentido, De Cupis (1975) sostiene que la intimidad constituye una manifestación de los derechos de la personalidad, orientada a preservar la esfera interna del individuo frente a cualquier forma de intromisión ilegítima. Esta protección se justifica en la necesidad de garantizar el respeto de la dignidad humana y el libre desarrollo de la personalidad.

Asimismo, el derecho a la intimidad personal y familiar se encuentra estrechamente vinculado con otros derechos fundamentales, como el derecho a la privacidad, el honor, la imagen y la protección de datos personales. Según Troncoso Reigada (2010), la intimidad protege el ámbito interno de la persona, mientras que la protección de datos personales se orienta al control de la información personal en el entorno social y digital. Esta relación evidencia la evolución de los mecanismos de protección jurídica frente a los riesgos derivados del desarrollo tecnológico y del tratamiento masivo de información.

En la sociedad contemporánea, el derecho a la intimidad personal y familiar adquiere especial relevancia debido al avance de las tecnologías de información, los sistemas de vigilancia y el procesamiento de datos personales. Estas herramientas pueden generar riesgos de intromisión en la vida privada de los individuos, lo que exige la existencia de mecanismos jurídicos eficaces que garanticen la protección de la esfera personal y familiar frente a posibles vulneraciones, especialmente en el ámbito de la actuación estatal.

2.2.2.3. Protección constitucional de la intimidad en el Perú

En el ordenamiento jurídico peruano, el derecho a la intimidad personal y familiar se encuentra reconocido expresamente en el artículo 2, inciso 7, de la Constitución Política del Perú de 1993, el cual establece que toda persona tiene derecho al honor, a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Este reconocimiento constitucional evidencia la importancia de la protección de la vida privada como garantía fundamental para el respeto de la dignidad humana y el libre desarrollo de la persona dentro del Estado constitucional de derecho (Eguiguren Praeli, 2019).

El Tribunal Constitucional peruano ha señalado que el derecho a la intimidad protege la esfera personal del individuo frente a cualquier forma de injerencia indebida por parte del Estado o de particulares. Asimismo, ha precisado que este derecho comprende el control sobre la información personal, la protección de las comunicaciones privadas y la inviolabilidad del ámbito personal y familiar. En este sentido, la jurisprudencia constitucional ha establecido que toda intervención en la esfera privada

debe estar debidamente justificada y respetar los principios de legalidad, razonabilidad y proporcionalidad (Landa Arroyo, 2017).

La protección constitucional de la intimidad también implica la obligación del Estado de adoptar medidas normativas e institucionales que garanticen la tutela efectiva de este derecho frente a posibles vulneraciones. Esta protección se materializa mediante mecanismos jurisdiccionales como el proceso de amparo y el hábeas data, los cuales permiten restablecer el ejercicio del derecho cuando este ha sido afectado por actos u omisiones de autoridades públicas o particulares.

Finalmente, la protección constitucional del derecho a la intimidad en el Perú adquiere especial relevancia en el contexto de la transformación digital y el uso de tecnologías de información por parte del Estado. El desarrollo de sistemas de vigilancia digital y el tratamiento masivo de datos personales generan nuevos desafíos para la protección de la vida privada, lo que exige el fortalecimiento del marco jurídico y de los mecanismos de tutela constitucional para garantizar el respeto de los derechos fundamentales en la sociedad contemporánea.

2.2.2.4. Relación entre intimidad, privacidad y datos personales

La relación entre el derecho a la intimidad, el derecho a la privacidad y el derecho a la protección de datos personales responde a la evolución de los mecanismos jurídicos destinados a proteger la esfera personal del individuo frente a las injerencias del Estado y de terceros. Estos derechos comparten como fundamento común la dignidad humana y la necesidad de garantizar la autonomía individual en el desarrollo de la personalidad. Según Pérez Luño (2016), el desarrollo tecnológico ha ampliado el ámbito de protección de la vida privada, dando lugar a nuevas formas de tutela jurídica que buscan preservar la información personal y la esfera íntima del individuo en las sociedades contemporáneas.

Desde una perspectiva conceptual, el derecho a la intimidad protege el ámbito más reservado de la vida personal y familiar del individuo, comprendiendo aspectos relacionados con sus relaciones personales, creencias, comunicaciones y vida privada. Por su parte, el derecho a la privacidad posee un alcance más amplio, pues comprende el control sobre la información personal y las relaciones sociales del individuo frente a posibles injerencias externas. En este sentido, Troncoso Reigada (2010) señala que la intimidad constituye el núcleo esencial de la vida privada, mientras que la privacidad

abarca un ámbito más extenso de protección relacionado con la gestión de la información personal en diferentes contextos sociales.

El derecho a la protección de datos personales surge como una manifestación específica del derecho a la privacidad, orientada a garantizar el control del individuo sobre el tratamiento de su información personal, especialmente en entornos digitales. Este derecho reconoce la facultad del titular de decidir sobre la recopilación, uso, almacenamiento y difusión de sus datos personales, lo que se vincula con el principio de autodeterminación informativa. Según Alexy (2007), los derechos fundamentales evolucionan conforme a las necesidades sociales y tecnológicas, lo que explica el reconocimiento progresivo del derecho a la protección de datos personales como garantía autónoma frente al tratamiento masivo de información.

Asimismo, la relación entre estos derechos evidencia un proceso de ampliación progresiva de la protección jurídica de la persona frente al desarrollo de tecnologías de información y sistemas de vigilancia. Mientras que la intimidad protege el ámbito interno del individuo, la privacidad regula el acceso a la información personal y la protección de datos personales garantiza el control sobre el tratamiento de dicha información. De esta manera, estos derechos se complementan entre sí, formando un sistema integral de protección de la esfera personal del individuo frente a posibles vulneraciones derivadas del uso indebido de información.

En el contexto del Estado constitucional de derecho, la protección conjunta de la intimidad, la privacidad y los datos personales resulta esencial para garantizar el respeto de la dignidad humana y el libre desarrollo de la personalidad. La evolución tecnológica y el uso de sistemas de vigilancia digital han incrementado los riesgos de afectación a estos derechos, lo que exige el fortalecimiento de los mecanismos jurídicos que aseguren su tutela efectiva, especialmente frente al tratamiento de información personal por parte de entidades públicas.

2.2.3. Derecho fundamental a la protección de datos personales

El derecho fundamental a la protección de datos personales constituye una garantía jurídica orientada a proteger la información personal del individuo frente a su tratamiento indebido por parte del Estado o de terceros. Este derecho tiene como finalidad garantizar el control del titular sobre sus datos personales, evitando su recopilación,

almacenamiento o difusión sin consentimiento o sin justificación legal. Según Davara Rodríguez (2014), la protección de datos personales se configura como un derecho autónomo que busca salvaguardar la libertad y la dignidad de la persona frente al desarrollo de tecnologías que permiten el tratamiento masivo de información.

Este derecho surge como respuesta a los riesgos derivados del avance tecnológico y del uso de sistemas automatizados de procesamiento de información, los cuales han incrementado la capacidad de recopilar, almacenar y utilizar datos personales. En este contexto, la protección de datos personales se convierte en un instrumento esencial para garantizar la autodeterminación informativa y el respeto de la vida privada del individuo en la sociedad digital. Como señala Frosini (1984), el desarrollo de la informática transformó las formas tradicionales de protección de la intimidad, generando la necesidad de establecer nuevos mecanismos jurídicos que regulen el tratamiento de la información personal.

Asimismo, el derecho a la protección de datos personales se vincula con la evolución del Estado constitucional y la expansión de los derechos fundamentales en respuesta a los cambios sociales y tecnológicos. Este derecho busca equilibrar el uso de tecnologías de información con la protección de la dignidad humana y la libertad individual. En este sentido, Martínez Martínez (2007) sostiene que la protección de datos personales constituye una manifestación moderna de los derechos de la personalidad, cuyo reconocimiento responde a la necesidad de regular el poder informático en las sociedades contemporáneas.

En el ordenamiento jurídico peruano, el derecho a la protección de datos personales ha adquirido relevancia constitucional y legal mediante su reconocimiento en la Constitución Política del Perú y su desarrollo en la Ley N.º 29733, Ley de Protección de Datos Personales. Esta regulación establece principios y mecanismos destinados a garantizar el tratamiento adecuado de la información personal, evidenciando la importancia de este derecho como garantía fundamental frente al uso de tecnologías digitales y sistemas de vigilancia en el ámbito público y privado.

2.2.3.1. Origen y evolución del derecho a la protección de datos personales

El origen del derecho a la protección de datos personales se encuentra vinculado al desarrollo tecnológico y al surgimiento de los sistemas automatizados de tratamiento

de información durante la segunda mitad del siglo XX. El uso creciente de bases de datos informáticas generó preocupaciones respecto al control de la información personal y los riesgos de vulneración de la privacidad, lo que motivó la creación de mecanismos jurídicos orientados a proteger los derechos de los individuos frente al procesamiento de datos. Según Frosini (1984), el desarrollo de la informática dio origen a una nueva dimensión del derecho a la privacidad, conocida como libertad informática, que reconoce la necesidad de proteger al individuo frente al poder informático.

Uno de los antecedentes más relevantes en la evolución de este derecho se encuentra en la legislación europea, particularmente en la Ley de Protección de Datos del Estado de Hesse en Alemania de 1970, considerada una de las primeras normas destinadas a regular el tratamiento automatizado de datos personales. Posteriormente, el Tribunal Constitucional Federal alemán, en su sentencia sobre el censo de 1983, reconoció el derecho a la autodeterminación informativa como garantía fundamental para el control de la información personal (Martínez Martínez, 2007). Este reconocimiento marcó un hito en la consolidación del derecho a la protección de datos personales como derecho fundamental autónomo.

Asimismo, el desarrollo del derecho a la protección de datos personales se consolidó a nivel internacional mediante instrumentos jurídicos orientados a regular el tratamiento de información personal y garantizar la protección de la privacidad en entornos digitales. En este contexto, la regulación europea ha desempeñado un papel fundamental en la evolución de este derecho, estableciendo principios como consentimiento, finalidad y proporcionalidad en el tratamiento de datos personales. Como señala Davara Rodríguez (2014), estas regulaciones han influido significativamente en los ordenamientos jurídicos de diversos países, promoviendo el reconocimiento del derecho a la protección de datos personales como garantía esencial de la libertad individual.

En América Latina y particularmente en el Perú, el reconocimiento del derecho a la protección de datos personales responde al proceso de constitucionalización de los derechos fundamentales y al impacto de la transformación digital en la sociedad. La Constitución Política del Perú reconoce el derecho a la protección de la información personal, mientras que la Ley N.º 29733 regula su tratamiento y establece mecanismos de tutela frente a su uso indebido. Esta evolución normativa evidencia la importancia de

garantizar la protección de los datos personales como respuesta a los desafíos derivados del uso de tecnologías de información y sistemas de vigilancia en la sociedad contemporánea.

2.2.3.2. Concepto de datos personales

Los datos personales constituyen toda información que permite identificar o hacer identificable a una persona natural, directa o indirectamente, a través de elementos como nombre, identidad, características físicas, información económica, ubicación, datos biométricos u otros aspectos vinculados a su identidad. Este concepto se fundamenta en la necesidad de proteger la información personal del individuo frente a su tratamiento indebido, especialmente en el contexto del desarrollo tecnológico y el uso masivo de sistemas de información. Según Davara Rodríguez (2014), los datos personales comprenden cualquier información relativa a una persona física identificada o identificable, cuyo tratamiento debe estar sujeto a garantías jurídicas que protejan los derechos fundamentales del titular.

Desde una perspectiva jurídica, los datos personales constituyen el objeto de protección del derecho fundamental a la protección de datos personales, en tanto representan información vinculada a la esfera privada del individuo. En este sentido, Martínez Martínez (2007) señala que los datos personales son manifestaciones de la identidad del individuo, cuya protección resulta esencial para garantizar la libertad personal, la dignidad humana y la autodeterminación informativa en la sociedad digital.

En el ordenamiento jurídico peruano, la Ley N.º 29733, Ley de Protección de Datos Personales, define los datos personales como toda información sobre una persona natural que la identifica o la hace identificable a través de medios razonablemente utilizables. Esta definición incluye datos sensibles relacionados con aspectos como origen racial o étnico, convicciones religiosas, información sobre la salud o datos biométricos, los cuales requieren un mayor nivel de protección debido a su potencial impacto en la esfera personal del individuo (Congreso de la República del Perú, 2011).

En la actualidad, el concepto de datos personales ha adquirido mayor relevancia debido al desarrollo de tecnologías digitales que permiten la recopilación, almacenamiento y procesamiento masivo de información. El uso de bases de datos, sistemas de vigilancia digital y plataformas electrónicas ha incrementado los riesgos de

tratamiento indebido de la información personal, lo que exige la existencia de mecanismos jurídicos que regulen su tratamiento y garanticen la protección efectiva de los derechos fundamentales del individuo.

2.2.3.3. Autodeterminación informativa

La autodeterminación informativa constituye un principio fundamental del derecho a la protección de datos personales, que reconoce la facultad del individuo de controlar la recopilación, uso, almacenamiento y difusión de su información personal. Este concepto surge como respuesta al desarrollo de tecnologías de información que incrementaron la capacidad de tratamiento automatizado de datos personales, generando la necesidad de garantizar el control del individuo sobre su información. Según Frosini (1984), la autodeterminación informativa representa la libertad del individuo frente al poder informático, permitiéndole decidir sobre el tratamiento de los datos que le conciernen.

El reconocimiento jurídico de la autodeterminación informativa tiene su origen en la jurisprudencia del Tribunal Constitucional Federal alemán, particularmente en la sentencia sobre el censo de 1983, en la cual se estableció que el individuo tiene derecho a decidir sobre la divulgación y uso de su información personal. Este derecho se configura como una garantía de la libertad individual y una manifestación del principio de dignidad humana frente al tratamiento automatizado de información (Martínez Martínez, 2007).

Desde una perspectiva doctrinaria, la autodeterminación informativa constituye una expresión del libre desarrollo de la personalidad y del derecho a la privacidad, en tanto permite al individuo controlar su identidad informativa y evitar el uso indebido de sus datos personales. Según Pérez Luño (2016), este principio garantiza la autonomía del individuo en el entorno digital y limita el poder del Estado y de terceros en el tratamiento de información personal, contribuyendo a la protección de los derechos fundamentales en la sociedad tecnológica.

En el contexto del Estado constitucional de derecho, la autodeterminación informativa se configura como un mecanismo esencial para garantizar el respeto de la dignidad humana y la protección de la vida privada frente al uso de tecnologías de información. Su reconocimiento implica la obligación del Estado de establecer normas y mecanismos de control que aseguren el tratamiento legítimo de los datos personales,

especialmente frente al uso de sistemas de vigilancia digital y procesamiento masivo de información en el sector público.

2.2.3.4.Principios del tratamiento de datos personales

El tratamiento de datos personales se rige por un conjunto de principios jurídicos orientados a garantizar el respeto del derecho fundamental a la protección de datos personales y la protección de la dignidad humana. Estos principios constituyen criterios rectores que regulan la recopilación, almacenamiento, uso y difusión de información personal, estableciendo límites al tratamiento de los datos y obligaciones para quienes los gestionan. Según Davara Rodríguez (2014), los principios del tratamiento de datos personales representan garantías jurídicas destinadas a asegurar el uso legítimo de la información personal y prevenir su tratamiento arbitrario o indebido.

En el ordenamiento jurídico peruano, la Ley N.º 29733, Ley de Protección de Datos Personales, establece principios fundamentales como legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad y disposición de recurso. El principio de legalidad establece que el tratamiento de datos personales debe realizarse conforme a la ley y respetando los derechos fundamentales del titular. Por su parte, el principio de consentimiento exige la autorización libre, previa, expresa e informada del titular para el tratamiento de sus datos personales, salvo excepciones previstas por la normativa (Congreso de la República del Perú, 2011).

Asimismo, el principio de finalidad establece que los datos personales deben ser recopilados para fines determinados, explícitos y legítimos, prohibiéndose su uso para propósitos distintos a aquellos para los cuales fueron obtenidos. El principio de proporcionalidad exige que el tratamiento de datos sea adecuado, relevante y no excesivo en relación con la finalidad que lo justifica. En este sentido, Martínez Martínez (2007) señala que estos principios buscan garantizar el equilibrio entre el tratamiento de información personal y la protección de los derechos fundamentales del individuo.

Finalmente, el principio de seguridad impone la obligación de adoptar medidas técnicas, organizativas y legales destinadas a proteger los datos personales frente a accesos no autorizados, pérdida o uso indebido. Estos principios constituyen mecanismos esenciales para garantizar el tratamiento responsable de la información personal,

especialmente en el contexto del desarrollo tecnológico y del uso de sistemas de vigilancia digital por parte del Estado y de entidades públicas.

2.2.3.5. Derechos del titular de datos personales

El derecho a la protección de datos personales reconoce al titular de los datos un conjunto de facultades orientadas a garantizar el control sobre su información personal y asegurar el respeto de su dignidad y libertad individual. Estos derechos permiten al individuo intervenir en el tratamiento de sus datos personales, evitando su uso indebido o arbitrario. Según Troncoso Reigada (2010), los derechos del titular constituyen mecanismos de tutela que garantizan la autodeterminación informativa y el control efectivo de la persona sobre su información personal.

En el ordenamiento jurídico peruano, la Ley N.º 29733 reconoce derechos fundamentales del titular de datos personales, entre los cuales destacan el derecho de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales. El derecho de acceso permite al titular conocer qué información personal está siendo tratada y con qué finalidad; el derecho de rectificación permite corregir datos inexactos o incompletos; el derecho de cancelación faculta a solicitar la eliminación de datos cuando su tratamiento resulte indebido; y el derecho de oposición permite impedir el tratamiento de datos cuando existan motivos legítimos para ello (Congreso de la República del Perú, 2011).

Asimismo, estos derechos garantizan la transparencia en el tratamiento de la información personal y establecen límites al poder de quienes gestionan datos personales. En este sentido, Davara Rodríguez (2014) sostiene que el reconocimiento de los derechos del titular constituye un elemento esencial del sistema de protección de datos personales, pues permite al individuo ejercer control sobre el tratamiento de su información y exigir responsabilidad frente a posibles vulneraciones.

Finalmente, los derechos del titular de datos personales se configuran como garantías fundamentales para la protección de la privacidad y la autodeterminación informativa en la sociedad digital. Su reconocimiento implica la obligación del Estado de establecer mecanismos efectivos para su ejercicio y tutela, especialmente frente al tratamiento masivo de información y al uso de sistemas tecnológicos por parte de

entidades públicas, garantizando así la protección de los derechos fundamentales en el Estado constitucional de derecho.

2.2.3.6. Protección constitucional del derecho a los datos personales en el Perú

En el ordenamiento jurídico peruano, el derecho a la protección de datos personales posee reconocimiento constitucional como parte del catálogo de derechos fundamentales orientados a garantizar la dignidad humana y la protección de la vida privada. La Constitución Política del Perú de 1993 establece en su artículo 2, inciso 6, que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte su intimidad personal y familiar. Este reconocimiento constitucional configura la base jurídica para la protección de los datos personales y establece límites al tratamiento de la información personal por parte del Estado y de terceros (Eguiguren Praeli, 2019).

Asimismo, la protección constitucional del derecho a los datos personales se vincula con otros derechos fundamentales, como el derecho a la intimidad personal y familiar, el honor, la buena reputación y el libre desarrollo de la personalidad, conformando un sistema integral de protección de la persona frente al tratamiento indebido de información. En este sentido, el Tribunal Constitucional peruano ha señalado que el derecho a la protección de datos personales constituye una manifestación del derecho a la autodeterminación informativa, que garantiza el control del individuo sobre la información que le concierne y limita el ejercicio del poder estatal en el tratamiento de datos personales (Landa Arroyo, 2017).

La protección constitucional de este derecho también se materializa a través de mecanismos jurisdiccionales destinados a garantizar su tutela efectiva frente a posibles vulneraciones. En el sistema jurídico peruano, el proceso constitucional de hábeas data constituye el principal mecanismo de protección del derecho a los datos personales, permitiendo al titular acceder a la información que le concierne, solicitar su actualización, rectificación o supresión cuando corresponda. Este mecanismo garantiza el control del individuo sobre su información personal y asegura la protección de sus derechos fundamentales frente al tratamiento indebido de datos (García Toma, 2013).

Por otro lado, el desarrollo legislativo del derecho a la protección de datos personales se concreta en la Ley N.º 29733, Ley de Protección de Datos Personales, y su

reglamento, los cuales establecen principios, obligaciones y mecanismos de tutela destinados a garantizar el tratamiento adecuado de la información personal. Esta normativa desarrolla el mandato constitucional y establece un sistema de protección jurídica orientado a regular el tratamiento de datos personales en el ámbito público y privado, evidenciando el proceso de constitucionalización del derecho a la protección de datos personales en el Perú (Congreso de la República del Perú, 2011).

Finalmente, la protección constitucional del derecho a los datos personales adquiere especial relevancia en el contexto de la transformación digital y el uso de tecnologías de información por parte del Estado. El desarrollo de sistemas de vigilancia digital, bases de datos interconectadas y mecanismos de tratamiento automatizado de información plantea nuevos desafíos para la protección de los derechos fundamentales, lo que exige el fortalecimiento del marco jurídico y de los mecanismos de control constitucional para garantizar la tutela efectiva de la dignidad humana y la libertad individual en la sociedad contemporánea.

2.2.4. Sistemas de vigilancia digital

Los sistemas de vigilancia digital constituyen mecanismos tecnológicos destinados a recopilar, almacenar y procesar información sobre las personas mediante el uso de herramientas digitales, redes informáticas y dispositivos electrónicos. Estos sistemas permiten el monitoreo de conductas, comunicaciones y datos personales con fines de seguridad, control administrativo o gestión pública. En el contexto de la sociedad contemporánea, la expansión de estas tecnologías ha generado importantes debates jurídicos sobre sus implicancias en la protección de los derechos fundamentales, especialmente el derecho a la privacidad y la protección de datos personales (Lyon, 2018).

El desarrollo de los sistemas de vigilancia digital se encuentra estrechamente vinculado al avance de las tecnologías de la información y la comunicación, que han ampliado la capacidad del Estado y de otras organizaciones para recopilar y analizar grandes volúmenes de datos personales. Según Zuboff (2019), la vigilancia digital representa una nueva forma de control social basada en la recopilación masiva de información personal mediante tecnologías digitales, lo que genera riesgos para la autonomía individual y la libertad personal.

Desde una perspectiva jurídica, los sistemas de vigilancia digital plantean tensiones entre la protección de la seguridad pública y el respeto de los derechos fundamentales. El uso de tecnologías de monitoreo por parte del Estado puede resultar legítimo cuando persigue fines de interés público, pero debe respetar los principios de legalidad, necesidad y proporcionalidad para evitar afectaciones indebidas a la esfera personal del individuo (Bygrave, 2014). En este sentido, la regulación jurídica de la vigilancia digital constituye un elemento esencial para garantizar el equilibrio entre el interés público y la protección de los derechos fundamentales.

En el ámbito del sector público, los sistemas de vigilancia digital adquieren especial relevancia debido al poder del Estado para recopilar y gestionar información personal de los ciudadanos. El uso de estas tecnologías exige el establecimiento de mecanismos de control y supervisión que aseguren el tratamiento legítimo de los datos personales y eviten prácticas de vigilancia excesiva que puedan afectar la dignidad humana y las libertades individuales en el Estado constitucional de derecho.

2.2.4.1. Concepto de vigilancia digital

La vigilancia digital puede definirse como el conjunto de prácticas y tecnologías destinadas a monitorear, registrar y analizar la información personal de los individuos mediante el uso de sistemas electrónicos, redes informáticas y dispositivos tecnológicos. Este concepto comprende el seguimiento de actividades, comunicaciones y comportamientos de las personas en entornos digitales o físicos mediante herramientas tecnológicas. Según Lyon (2018), la vigilancia digital consiste en la recopilación sistemática de información personal con el propósito de influir, gestionar o controlar conductas humanas.

Desde una perspectiva sociológica y jurídica, la vigilancia digital implica el uso de tecnologías de información para observar y registrar datos sobre los individuos con fines de seguridad, administración o control social. En este sentido, Foucault (2002) explica que los mecanismos de vigilancia constituyen formas de ejercicio del poder que permiten supervisar la conducta de las personas mediante sistemas de control, lo que ha sido adaptado en la actualidad al uso de tecnologías digitales.

Asimismo, la vigilancia digital se caracteriza por su capacidad de recopilación masiva y automatizada de información personal, lo que permite la elaboración de perfiles

individuales y el análisis de comportamientos mediante algoritmos y sistemas informáticos. Según Zuboff (2019), las tecnologías digitales han transformado la vigilancia tradicional en sistemas de monitoreo permanente basados en el tratamiento masivo de datos personales.

En el ámbito jurídico, el concepto de vigilancia digital se relaciona con el tratamiento de datos personales y la protección de la privacidad, ya que implica la recopilación y procesamiento de información que puede afectar la esfera personal del individuo. Por ello, su regulación debe garantizar el respeto de los derechos fundamentales y establecer límites al uso de tecnologías de monitoreo por parte del Estado y de otras entidades.

2.2.4.2. Tipos de sistemas de vigilancia digital

Los sistemas de vigilancia digital pueden clasificarse en diversas categorías según las tecnologías empleadas y los fines perseguidos. Uno de los principales tipos es la videovigilancia, que consiste en el uso de cámaras de seguridad y sistemas de grabación para monitorear espacios públicos o privados. Según Lyon (2018), la videovigilancia constituye uno de los mecanismos más extendidos de vigilancia digital, debido a su capacidad para registrar comportamientos y generar información visual sobre las personas.

Otro tipo relevante es la vigilancia biométrica, que utiliza características físicas o biológicas de los individuos, como huellas dactilares, reconocimiento facial o escaneo del iris, para identificar o autenticar a las personas. Este tipo de vigilancia permite el tratamiento de datos sensibles y plantea importantes desafíos para la protección de los derechos fundamentales, debido a su carácter invasivo y su potencial impacto en la privacidad y la identidad personal (Bygrave, 2014).

Asimismo, existen sistemas de vigilancia digital basados en el monitoreo de comunicaciones electrónicas y actividades en línea, como la interceptación de comunicaciones, el seguimiento de navegación en internet y el análisis de datos en redes digitales. Estos sistemas permiten recopilar información sobre las actividades y comportamientos de los individuos en el entorno digital, lo que genera riesgos para la privacidad y la protección de datos personales (Zuboff, 2019).

Finalmente, los sistemas de vigilancia digital también comprenden el uso de bases de datos interconectadas y tecnologías de análisis masivo de información, conocidas como big data, que permiten procesar grandes volúmenes de datos personales para fines de seguridad, gestión pública o control administrativo. Estos sistemas incrementan la capacidad de monitoreo del Estado y requieren mecanismos jurídicos adecuados que garanticen el respeto de los derechos fundamentales y eviten el uso arbitrario de la información personal.

2.2.4.3. Vigilancia estatal y seguridad pública

La vigilancia estatal constituye una actividad mediante la cual el Estado emplea mecanismos tecnológicos y administrativos para supervisar conductas, prevenir delitos y garantizar la seguridad pública. Esta función se fundamenta en la obligación del Estado de proteger el orden público y la seguridad ciudadana, lo que justifica el uso de herramientas de monitoreo y control en determinados contextos. Según Lyon (2018), la vigilancia estatal se configura como una práctica institucional orientada a la gestión del riesgo y la protección de la seguridad colectiva, especialmente en sociedades contemporáneas caracterizadas por el uso intensivo de tecnologías digitales.

Desde una perspectiva jurídica, la vigilancia estatal debe ejercerse dentro del marco del respeto a los derechos fundamentales y conforme a los principios de legalidad, necesidad y proporcionalidad. El uso de sistemas de vigilancia por parte del Estado puede resultar legítimo cuando responde a fines constitucionalmente válidos, como la prevención del delito o la protección de la seguridad pública; sin embargo, su aplicación debe evitar intervenciones arbitrarias en la esfera privada de los ciudadanos. En este sentido, Solove (2021) sostiene que las políticas de vigilancia estatal requieren mecanismos de control jurídico que garanticen la protección de la privacidad y limiten el ejercicio del poder público.

Asimismo, la relación entre vigilancia estatal y seguridad pública plantea tensiones entre el interés colectivo y los derechos individuales. El fortalecimiento de mecanismos de control estatal puede contribuir a la seguridad ciudadana, pero también puede generar riesgos de vigilancia excesiva, control social y afectación de libertades fundamentales. Según Zedner (2009), la expansión de políticas de seguridad basadas en

vigilancia tecnológica puede conducir a un aumento del poder estatal, lo que exige la existencia de límites jurídicos claros para evitar abusos.

En el contexto del Estado constitucional de derecho, la vigilancia estatal debe estar sujeta a mecanismos de control institucional y jurisdiccional que aseguren su legitimidad y eviten vulneraciones a los derechos fundamentales. La regulación jurídica de la vigilancia estatal constituye un elemento esencial para garantizar el equilibrio entre la protección de la seguridad pública y el respeto de la dignidad humana, especialmente frente al uso de tecnologías digitales que incrementan la capacidad de monitoreo del Estado.

2.2.4.4. Impacto de la vigilancia digital en los derechos fundamentales

El desarrollo de la vigilancia digital ha generado importantes implicancias en la protección de los derechos fundamentales, particularmente en relación con el derecho a la privacidad, la intimidad y la protección de datos personales. El uso de tecnologías de monitoreo permite la recopilación masiva de información personal, lo que puede afectar la autonomía individual y el libre desarrollo de la personalidad. Según Zuboff (2019), la expansión de sistemas de vigilancia digital ha transformado las relaciones entre el individuo y las instituciones, generando nuevos riesgos para la libertad individual en la sociedad contemporánea.

Uno de los principales efectos de la vigilancia digital es la posible afectación del derecho a la privacidad, debido al acceso constante a información personal y al monitoreo de las actividades de los individuos. En este sentido, Solove (2021) sostiene que la vigilancia digital puede generar riesgos de invasión de la esfera privada, perfilamiento de conductas y uso indebido de información personal, lo que exige mecanismos jurídicos que garanticen la protección de los derechos fundamentales.

Asimismo, la vigilancia digital puede afectar otros derechos fundamentales, como la libertad de expresión, la libertad de asociación y el derecho a la autodeterminación informativa. El monitoreo permanente de las actividades de los individuos puede generar efectos inhibitorios en el ejercicio de estos derechos, limitando la participación ciudadana y el ejercicio de las libertades públicas. Según Lyon (2018), la vigilancia sistemática puede producir cambios en el comportamiento social de los individuos debido a la percepción de control permanente.

Finalmente, el impacto de la vigilancia digital en los derechos fundamentales exige el establecimiento de mecanismos jurídicos de regulación y control que garanticen el respeto de la dignidad humana y la protección de las libertades individuales. En el Estado constitucional de derecho, la implementación de sistemas de vigilancia debe estar sujeta a principios de proporcionalidad, transparencia y responsabilidad, a fin de asegurar un equilibrio adecuado entre el uso de tecnologías digitales y la protección de los derechos fundamentales.

2.2.5. Tratamiento de datos personales en el sector público

El tratamiento de datos personales en el sector público comprende el conjunto de operaciones realizadas por entidades estatales destinadas a la recopilación, almacenamiento, procesamiento, transmisión y uso de información personal de los ciudadanos en el ejercicio de sus funciones administrativas. Este tratamiento se justifica en la necesidad de garantizar la prestación de servicios públicos, la gestión administrativa y la seguridad del Estado; sin embargo, debe realizarse respetando los derechos fundamentales de las personas. Según Bygrave (2014), el tratamiento de datos personales por entidades públicas exige un marco jurídico que establezca límites claros al ejercicio del poder estatal y garantice la protección de la información personal.

En el ordenamiento jurídico peruano, el tratamiento de datos personales en el sector público se encuentra regulado por la Ley N.º 29733, Ley de Protección de Datos Personales, la cual establece principios y obligaciones que deben ser observados por las entidades públicas en el manejo de información personal. Esta normativa impone el deber de garantizar el tratamiento legítimo de los datos personales, respetando principios como legalidad, finalidad, proporcionalidad y seguridad en el uso de la información (Congreso de la República del Perú, 2011).

Asimismo, el tratamiento de datos personales por parte de la administración pública se caracteriza por la existencia de una relación asimétrica entre el Estado y el ciudadano, debido al poder que posee el Estado para recopilar grandes volúmenes de información personal. En este sentido, Cotino Hueso (2015) señala que el uso de tecnologías digitales por parte de la administración pública incrementa la capacidad de tratamiento de datos personales, lo que exige el fortalecimiento de mecanismos de control y protección de los derechos fundamentales.

En el contexto de la transformación digital del Estado, el tratamiento de datos personales en el sector público adquiere especial relevancia debido al uso de sistemas informáticos, bases de datos interconectadas y mecanismos de vigilancia digital. Estas prácticas generan desafíos jurídicos relacionados con la protección de la privacidad, la transparencia en la gestión pública y la protección de los derechos fundamentales, lo que exige una regulación adecuada que garantice el equilibrio entre la eficiencia administrativa y el respeto de la dignidad humana.

2.2.5.1. Administración pública y tratamiento de datos personales

La administración pública desempeña un papel fundamental en el tratamiento de datos personales, debido a que gestiona información de los ciudadanos para el cumplimiento de funciones administrativas, prestación de servicios públicos y formulación de políticas públicas. El tratamiento de datos personales en este ámbito constituye una actividad necesaria para el funcionamiento del Estado; sin embargo, debe realizarse conforme a principios jurídicos que garanticen la protección de los derechos fundamentales. Según Cassese (2016), la administración pública moderna se caracteriza por el uso intensivo de información como instrumento de gestión, lo que incrementa la importancia de regular el tratamiento de datos personales.

Desde una perspectiva jurídica, el tratamiento de datos personales por la administración pública debe regirse por el principio de legalidad, lo que implica que toda actividad de tratamiento debe estar autorizada por una norma jurídica y orientada al cumplimiento de fines legítimos. Asimismo, la actuación administrativa debe respetar los principios de transparencia, responsabilidad y protección de los derechos fundamentales en el manejo de la información personal (Cotino Hueso, 2015).

En el ordenamiento jurídico peruano, las entidades públicas tienen la obligación de garantizar la protección de los datos personales que administran, adoptando medidas técnicas y organizativas destinadas a prevenir el acceso no autorizado, el uso indebido o la divulgación de la información personal. Esta obligación responde al deber del Estado de proteger la dignidad humana y garantizar el respeto de los derechos fundamentales en el ejercicio de la función administrativa (Congreso de la República del Perú, 2011).

Finalmente, el tratamiento de datos personales en la administración pública debe orientarse a garantizar la eficiencia en la gestión pública sin afectar los derechos

fundamentales de los ciudadanos. El uso de tecnologías digitales en la gestión administrativa exige el establecimiento de mecanismos de control y supervisión que aseguren el tratamiento legítimo de la información personal y prevengan posibles abusos en el ejercicio del poder estatal.

2.2.5.2. Límites del poder estatal en el tratamiento de datos

El poder del Estado en el tratamiento de datos personales no es absoluto, sino que se encuentra sujeto a límites jurídicos destinados a garantizar la protección de los derechos fundamentales y evitar el uso arbitrario de la información personal. Estos límites se fundamentan en el principio del Estado constitucional de derecho, que establece que toda actuación estatal debe respetar la dignidad humana y los derechos fundamentales de los ciudadanos. Según Ferrajoli (2011), el ejercicio del poder público debe estar sometido a garantías jurídicas que impidan la vulneración de los derechos individuales.

Uno de los principales límites al tratamiento de datos personales por parte del Estado es el principio de legalidad, que exige que toda actividad de tratamiento se realice conforme a la ley y dentro de los fines establecidos por el ordenamiento jurídico. Asimismo, el principio de proporcionalidad establece que el tratamiento de datos personales debe ser adecuado, necesario y razonable en relación con la finalidad que lo justifica, evitando intervenciones excesivas en la esfera personal del individuo (Bernal Pulido, 2007).

Asimismo, el poder estatal en el tratamiento de datos personales se encuentra limitado por el derecho a la autodeterminación informativa, que reconoce la facultad del individuo de controlar su información personal y oponerse a su tratamiento indebido. En este sentido, Bygrave (2014) sostiene que la protección de datos personales constituye un mecanismo de control del poder estatal en el manejo de información personal, garantizando la protección de la privacidad y la libertad individual.

Finalmente, los límites al poder estatal en el tratamiento de datos personales requieren la existencia de mecanismos de control institucional y jurisdiccional que garanticen la protección de los derechos fundamentales frente a posibles abusos. Estos mecanismos incluyen el control judicial, la supervisión administrativa y el reconocimiento de derechos del titular de los datos, lo que permite asegurar el tratamiento

legítimo de la información personal y el respeto de la dignidad humana en el ejercicio de la función pública.

2.2.5.3. Garantías jurídicas en el tratamiento de datos personales

Las garantías jurídicas en el tratamiento de datos personales constituyen mecanismos normativos e institucionales orientados a proteger la información personal del individuo frente a su uso indebido, asegurando el respeto de los derechos fundamentales en el manejo de datos por parte de entidades públicas y privadas. Estas garantías tienen como finalidad establecer límites al tratamiento de datos personales, garantizar la transparencia en su gestión y proteger la dignidad humana frente al uso de tecnologías de información. Según Bygrave (2014), las garantías jurídicas en materia de protección de datos personales constituyen instrumentos esenciales para controlar el tratamiento de información y prevenir vulneraciones a la privacidad.

En el ordenamiento jurídico peruano, la Ley N.º 29733, Ley de Protección de Datos Personales, establece diversas garantías jurídicas orientadas a asegurar el tratamiento legítimo de la información personal. Entre estas garantías destacan el respeto de los principios del tratamiento de datos personales, la obligación de obtener el consentimiento del titular, la adopción de medidas de seguridad para proteger la información y el reconocimiento de derechos al titular de los datos. Estas disposiciones buscan garantizar que el tratamiento de datos personales se realice conforme al respeto de los derechos fundamentales y dentro de los límites establecidos por la ley (Congreso de la República del Perú, 2011).

Asimismo, las garantías jurídicas en el tratamiento de datos personales comprenden mecanismos institucionales de supervisión y control destinados a verificar el cumplimiento de la normativa sobre protección de datos personales. En el Perú, la Autoridad Nacional de Protección de Datos Personales ejerce funciones de supervisión, fiscalización y sanción respecto del tratamiento de datos personales, lo que contribuye a asegurar la protección efectiva de los derechos de los ciudadanos frente al manejo indebido de información personal (Cotino Hueso, 2015).

Finalmente, las garantías jurídicas en el tratamiento de datos personales también incluyen mecanismos jurisdiccionales de tutela, como el proceso constitucional de hábeas data, que permite al titular acceder a su información personal y exigir su rectificación,

actualización o supresión cuando corresponda. Estas garantías constituyen elementos esenciales del Estado constitucional de derecho, al asegurar el respeto de la dignidad humana y la protección de los derechos fundamentales frente al tratamiento de datos personales en el contexto de la transformación digital.

2.2.5.4. Responsabilidad del Estado en el uso de datos personales

La responsabilidad del Estado en el uso de datos personales se fundamenta en el deber de garantizar el respeto de los derechos fundamentales y asegurar el tratamiento legítimo de la información personal en el ejercicio de la función pública. El Estado, como titular de amplias facultades de recopilación y gestión de información, debe actuar conforme a los principios de legalidad, transparencia y protección de la dignidad humana. Según Cassese (2016), la actuación de la administración pública debe someterse a controles jurídicos que aseguren la protección de los derechos de los ciudadanos frente al ejercicio del poder estatal.

Desde una perspectiva jurídica, la responsabilidad del Estado en el tratamiento de datos personales implica la obligación de prevenir, controlar y sancionar el uso indebido de la información personal. El incumplimiento de las normas sobre protección de datos personales puede generar responsabilidad administrativa, civil o constitucional cuando se vulneran derechos fundamentales de los ciudadanos. En este sentido, Ferrajoli (2011) sostiene que el ejercicio del poder público debe estar sujeto a garantías jurídicas que permitan exigir responsabilidad frente a posibles abusos.

En el ordenamiento jurídico peruano, la responsabilidad del Estado en el uso de datos personales se encuentra vinculada al deber constitucional de proteger los derechos fundamentales y garantizar la legalidad en la actuación administrativa. La Ley N.º 29733 establece obligaciones para las entidades públicas respecto del tratamiento de datos personales, imponiendo sanciones en caso de incumplimiento y estableciendo mecanismos de tutela para los titulares de los datos (Congreso de la República del Perú, 2011).

Finalmente, la responsabilidad del Estado en el uso de datos personales adquiere especial relevancia en el contexto de la transformación digital y el uso de sistemas de vigilancia digital en la administración pública. El incremento del tratamiento automatizado de información exige el fortalecimiento de mecanismos de control y

responsabilidad estatal que garanticen la protección de la privacidad, la transparencia en la gestión pública y el respeto de los derechos fundamentales en el Estado constitucional de derecho.

2.2.6. Gobierno digital y transformación digital del Estado

El gobierno digital constituye una política pública orientada a la incorporación de tecnologías de la información y comunicación en la gestión pública con el objetivo de mejorar la eficiencia administrativa, la prestación de servicios públicos y la relación entre el Estado y los ciudadanos. Este proceso implica el uso de plataformas digitales, sistemas informáticos y bases de datos interconectadas para optimizar la toma de decisiones y la gestión administrativa. Según Gil-García, Helbig y Ojo (2014), el gobierno digital representa la transformación de las estructuras y procesos del Estado mediante el uso estratégico de tecnologías digitales para mejorar la gobernanza y la gestión pública.

La transformación digital del Estado supone un cambio estructural en la forma en que las instituciones públicas gestionan la información y prestan servicios a la ciudadanía. Este proceso implica la digitalización de procedimientos administrativos, el uso de sistemas de información interconectados y la implementación de mecanismos electrónicos de atención al ciudadano. En este sentido, Criado y Ramilo (2003) sostienen que la transformación digital del sector público implica la reorganización de la administración estatal mediante el uso de tecnologías digitales para mejorar la eficiencia y transparencia de la gestión pública.

Asimismo, el gobierno digital genera nuevas oportunidades para el fortalecimiento de la gestión pública, la transparencia administrativa y la participación ciudadana. El uso de tecnologías digitales permite mejorar el acceso a la información pública, optimizar los servicios estatales y fortalecer los mecanismos de control institucional. Sin embargo, este proceso también plantea desafíos jurídicos relacionados con la protección de datos personales, la seguridad de la información y el respeto de los derechos fundamentales.

En el contexto del Estado constitucional de derecho, la transformación digital del Estado debe desarrollarse dentro del marco del respeto de los derechos fundamentales y de los principios de legalidad, transparencia y responsabilidad. La incorporación de tecnologías digitales en la gestión pública exige la existencia de mecanismos jurídicos

adecuados que garanticen el tratamiento legítimo de la información personal y la protección de la dignidad humana frente al uso de sistemas tecnológicos.

2.2.6.1. Concepto de gobierno digital

El gobierno digital puede definirse como el uso estratégico de tecnologías de la información y comunicación por parte del Estado para mejorar la prestación de servicios públicos, optimizar la gestión administrativa y fortalecer la relación entre el Estado y los ciudadanos. Este concepto implica la digitalización de procesos administrativos, el uso de plataformas electrónicas y la implementación de sistemas informáticos para la gestión de la información pública. Según Naciones Unidas (2022), el gobierno digital constituye un modelo de gestión pública basado en el uso de tecnologías digitales para mejorar la eficiencia, transparencia y participación ciudadana.

Desde una perspectiva jurídica, el gobierno digital implica la adaptación del ordenamiento jurídico a los cambios derivados del uso de tecnologías digitales en la administración pública. Este proceso requiere el establecimiento de normas que regulen el tratamiento de datos personales, la seguridad de la información y la protección de los derechos fundamentales en el entorno digital. En este sentido, Cotino Hueso (2015) sostiene que el gobierno digital exige el desarrollo de un marco jurídico que garantice el respeto de los derechos fundamentales frente al uso de tecnologías en la gestión pública.

Asimismo, el gobierno digital se caracteriza por la utilización de herramientas tecnológicas como plataformas electrónicas, sistemas de identificación digital, bases de datos interconectadas y mecanismos de intercambio de información entre entidades públicas. Estas herramientas permiten mejorar la eficiencia de la gestión pública, pero también incrementan la capacidad del Estado para recopilar y procesar información personal, lo que genera desafíos para la protección de la privacidad y los datos personales.

En el Perú, el gobierno digital se encuentra vinculado al proceso de modernización del Estado y a la implementación de políticas públicas orientadas a la digitalización de los servicios administrativos. Este proceso implica la incorporación de tecnologías digitales en la gestión pública, lo que exige el fortalecimiento de mecanismos jurídicos que garanticen la protección de los derechos fundamentales en el entorno digital.

2.2.6.2.Modernización del Estado y uso de tecnologías digitales

La modernización del Estado constituye un proceso orientado a mejorar la eficiencia, transparencia y calidad de la gestión pública mediante la incorporación de nuevas tecnologías y modelos de administración. Este proceso implica la adopción de herramientas digitales para optimizar la prestación de servicios públicos, simplificar procedimientos administrativos y mejorar la relación entre el Estado y la ciudadanía. Según Criado (2016), la modernización del sector público se caracteriza por la integración de tecnologías digitales en la gestión administrativa como instrumento de innovación institucional.

El uso de tecnologías digitales en la administración pública permite mejorar la eficiencia en la gestión de la información, facilitar el acceso a servicios públicos y fortalecer la transparencia en la actuación estatal. Sin embargo, la incorporación de tecnologías digitales también incrementa la capacidad del Estado para recopilar y procesar grandes volúmenes de datos personales, lo que genera desafíos para la protección de la privacidad y los derechos fundamentales.

Asimismo, la modernización del Estado mediante tecnologías digitales implica el desarrollo de sistemas de información interconectados, plataformas electrónicas y mecanismos de intercambio de datos entre entidades públicas. Según Gil-García et al. (2014), la transformación digital del Estado requiere la adopción de políticas públicas orientadas a regular el uso de tecnologías digitales y garantizar la protección de los derechos de los ciudadanos.

En el Estado constitucional de derecho, el proceso de modernización estatal debe desarrollarse dentro del marco del respeto de los derechos fundamentales, garantizando la protección de la información personal y la transparencia en la gestión pública. La incorporación de tecnologías digitales exige el fortalecimiento del marco jurídico y de los mecanismos de control institucional para evitar abusos en el tratamiento de datos personales.

2.2.6.3.Riesgos jurídicos del tratamiento masivo de datos

El tratamiento masivo de datos personales constituye una práctica vinculada al uso de tecnologías digitales que permite la recopilación, almacenamiento y análisis de

grandes volúmenes de información personal. Este fenómeno plantea importantes riesgos jurídicos relacionados con la protección de la privacidad, la seguridad de la información y la protección de los derechos fundamentales. Según Mayer-Schönberger y Cukier (2013), el uso del big data permite procesar grandes cantidades de información personal, lo que puede generar riesgos de control social y afectación de la libertad individual.

Uno de los principales riesgos del tratamiento masivo de datos es la posible vulneración del derecho a la privacidad y la protección de datos personales mediante el uso indebido de información personal. El procesamiento automatizado de datos permite la elaboración de perfiles individuales y el monitoreo de conductas, lo que puede generar discriminación, exclusión social y afectación de derechos fundamentales (Zuboff, 2019).

Asimismo, el tratamiento masivo de datos plantea riesgos relacionados con la seguridad de la información, como el acceso no autorizado, la filtración de datos y el uso indebido de información personal. Según Bygrave (2014), el manejo de grandes volúmenes de datos personales exige la implementación de mecanismos jurídicos y técnicos destinados a garantizar la protección de la información y prevenir vulneraciones a los derechos fundamentales.

Finalmente, los riesgos jurídicos del tratamiento masivo de datos evidencian la necesidad de establecer marcos normativos adecuados que regulen el uso de tecnologías digitales en la gestión pública y garanticen la protección de la dignidad humana. En el contexto del Estado constitucional de derecho, el uso de tecnologías de información debe estar sujeto a principios de legalidad, proporcionalidad y responsabilidad, a fin de asegurar el respeto de los derechos fundamentales en la sociedad digital.

2.2.7. Tutela jurídica del derecho a la protección de datos personales

La tutela jurídica del derecho a la protección de datos personales comprende el conjunto de mecanismos constitucionales, legales e institucionales destinados a garantizar la protección efectiva de la información personal frente a su tratamiento indebido. Esta tutela constituye una garantía esencial del Estado constitucional de derecho, orientada a proteger la dignidad humana, la privacidad y la libertad individual frente al uso de tecnologías de información. Según Rebollo Delgado (2010), la tutela jurídica de los datos personales implica la existencia de mecanismos normativos y jurisdiccionales que permitan prevenir, controlar y sancionar el tratamiento ilícito de la información personal.

El derecho a la protección de datos personales requiere mecanismos de protección eficaces debido al incremento del tratamiento automatizado de información y al uso de sistemas digitales por parte de entidades públicas y privadas. En este sentido, González Fuster (2014) sostiene que la protección de datos personales constituye un elemento esencial de los sistemas democráticos, ya que garantiza el control del individuo sobre su información personal y limita el poder estatal en el manejo de datos.

Asimismo, la tutela jurídica de este derecho se manifiesta mediante garantías constitucionales, mecanismos jurisdiccionales de control, organismos administrativos de supervisión y procedimientos de protección frente a vulneraciones. Estos instrumentos permiten asegurar el cumplimiento de las normas sobre protección de datos personales y garantizar la reparación de los derechos afectados.

En el ordenamiento jurídico peruano, la tutela jurídica del derecho a la protección de datos personales se encuentra reconocida constitucionalmente y desarrollada mediante la Ley N.º 29733, así como mediante mecanismos de control jurisdiccional y supervisión administrativa que garantizan la protección efectiva de los derechos fundamentales frente al tratamiento indebido de información personal.

2.2.7.1. Garantías constitucionales

Las garantías constitucionales del derecho a la protección de datos personales constituyen mecanismos destinados a asegurar la protección efectiva de los derechos fundamentales reconocidos en la Constitución. Estas garantías tienen como finalidad proteger la dignidad humana, la privacidad y la autodeterminación informativa frente a posibles vulneraciones derivadas del tratamiento indebido de datos personales. Según Carbonell (2013), las garantías constitucionales representan instrumentos jurídicos orientados a asegurar la eficacia de los derechos fundamentales frente al ejercicio del poder público.

En el ordenamiento jurídico peruano, las garantías constitucionales del derecho a la protección de datos personales se fundamentan en el reconocimiento de este derecho en la Constitución Política del Perú y en la existencia de mecanismos procesales destinados a su protección. Estas garantías establecen límites al poder estatal y aseguran el respeto de los derechos fundamentales en el tratamiento de información personal.

Asimismo, las garantías constitucionales comprenden el principio de supremacía constitucional, el control de constitucionalidad y la existencia de procesos constitucionales destinados a restablecer el ejercicio de derechos vulnerados. En este sentido, Sagüés (2011) señala que las garantías constitucionales constituyen instrumentos de control del poder estatal y mecanismos de protección de los derechos fundamentales en el Estado constitucional de derecho.

Finalmente, las garantías constitucionales del derecho a la protección de datos personales adquieren especial relevancia en el contexto de la transformación digital, debido al incremento del tratamiento automatizado de información personal. Estas garantías permiten asegurar el respeto de los derechos fundamentales frente al uso de tecnologías digitales y el ejercicio del poder estatal.

2.2.7.2. Control jurisdiccional

El control jurisdiccional constituye un mecanismo esencial para la protección del derecho a la protección de datos personales, ya que permite a los órganos judiciales garantizar el respeto de los derechos fundamentales frente a actos u omisiones que vulneren la información personal de los individuos. Este control implica la intervención del poder judicial en la resolución de conflictos relacionados con el tratamiento de datos personales y la tutela de derechos fundamentales. Según Zagrebelsky (2008), el control jurisdiccional constituye una garantía esencial del Estado constitucional, al asegurar la protección efectiva de los derechos frente al ejercicio del poder.

En el ordenamiento jurídico peruano, el control jurisdiccional del derecho a la protección de datos personales se materializa mediante procesos constitucionales como el hábeas data, que permite al titular acceder a su información personal y exigir su rectificación o supresión. Este mecanismo garantiza el control del individuo sobre sus datos personales y asegura la tutela efectiva de sus derechos fundamentales.

Asimismo, el control jurisdiccional permite verificar la legalidad del tratamiento de datos personales y sancionar posibles vulneraciones a los derechos fundamentales. En este sentido, Prieto Sanchís (2003) sostiene que el control jurisdiccional constituye un instrumento esencial para garantizar la supremacía de la Constitución y la protección de los derechos fundamentales frente al poder público.

Finalmente, el control jurisdiccional del tratamiento de datos personales contribuye a fortalecer la protección de la privacidad y la seguridad jurídica en el uso de tecnologías digitales. Este mecanismo permite restablecer el ejercicio de derechos vulnerados y garantizar la responsabilidad de las entidades que realizan tratamiento indebido de información personal.

2.2.7.3. Autoridad Nacional de Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales constituye el órgano administrativo encargado de supervisar, fiscalizar y garantizar el cumplimiento de la normativa sobre protección de datos personales. Su función principal es asegurar el tratamiento legítimo de la información personal y proteger los derechos fundamentales de los ciudadanos frente al uso indebido de datos personales. Según Greenleaf (2014), las autoridades de protección de datos desempeñan un papel fundamental en la supervisión del cumplimiento de las normas sobre privacidad y en la protección de los derechos de los individuos.

En el Perú, la Autoridad Nacional de Protección de Datos Personales funciona como órgano del Ministerio de Justicia y Derechos Humanos, encargado de supervisar el cumplimiento de la Ley N.º 29733 y su reglamento. Esta entidad ejerce funciones de fiscalización, sanción y orientación en materia de tratamiento de datos personales, contribuyendo a garantizar la protección efectiva de los derechos fundamentales.

Asimismo, la actuación de la Autoridad Nacional de Protección de Datos Personales permite fortalecer la transparencia en el tratamiento de información personal y prevenir vulneraciones a la privacidad. Según Bennett y Raab (2006), las autoridades de protección de datos constituyen mecanismos institucionales esenciales para la protección de la información personal en las sociedades contemporáneas.

Finalmente, la existencia de organismos especializados en protección de datos personales evidencia el proceso de institucionalización de la tutela del derecho a la privacidad y la protección de datos en el Estado constitucional de derecho, garantizando el control del tratamiento de información personal en el ámbito público y privado.

2.2.7.4. Mecanismos de protección frente a vulneraciones

Los mecanismos de protección frente a vulneraciones del derecho a la protección de datos personales comprenden procedimientos jurídicos destinados a prevenir, sancionar y reparar el tratamiento indebido de información personal. Estos mecanismos permiten garantizar el ejercicio efectivo de los derechos fundamentales y asegurar la responsabilidad de quienes incumplen la normativa sobre protección de datos personales. Según González Fuster (2014), los mecanismos de protección constituyen elementos esenciales para garantizar la eficacia del derecho a la protección de datos personales.

Entre los principales mecanismos de protección se encuentran los procedimientos administrativos ante las autoridades de protección de datos, las acciones judiciales destinadas a restablecer el ejercicio de derechos vulnerados y los mecanismos de reparación frente al tratamiento indebido de información personal. Estos instrumentos permiten garantizar la protección efectiva de los derechos fundamentales en el entorno digital.

Asimismo, los mecanismos de protección frente a vulneraciones del derecho a la protección de datos personales incluyen medidas preventivas, correctivas y sancionadoras destinadas a evitar el uso indebido de información personal. En este sentido, Rebollo Delgado (2010) sostiene que la protección efectiva de los datos personales requiere la existencia de mecanismos de control que permitan prevenir vulneraciones y garantizar la responsabilidad de quienes realizan tratamiento ilícito de información.

Finalmente, la existencia de mecanismos de protección frente a vulneraciones del derecho a la protección de datos personales contribuye a fortalecer la seguridad jurídica y el respeto de los derechos fundamentales en el Estado constitucional de derecho. Estos mecanismos resultan especialmente relevantes en el contexto del uso de tecnologías digitales y sistemas de vigilancia que incrementan los riesgos de tratamiento indebido de información personal.

2.3.Marco normativo

2.3.1.Constitución Política del Perú

La Constitución Política del Perú de 1993 constituye la norma suprema del ordenamiento jurídico peruano y establece el reconocimiento y protección de los derechos

fundamentales de la persona, incluyendo el derecho a la protección de datos personales y el derecho a la intimidad. En particular, el artículo 2, inciso 6, reconoce el derecho de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte su intimidad personal y familiar, lo que constituye el fundamento constitucional de la protección de datos personales en el Perú.

Asimismo, el artículo 2, inciso 7, reconoce el derecho al honor, a la buena reputación y a la intimidad personal y familiar, mientras que el artículo 200 establece los procesos constitucionales destinados a la tutela de los derechos fundamentales, entre ellos el proceso de hábeas data, que garantiza el acceso, control y protección de la información personal. Estas disposiciones evidencian la existencia de un sistema constitucional orientado a la protección de la dignidad humana y la privacidad.

Desde una perspectiva doctrinaria, la Constitución establece límites al ejercicio del poder estatal en el tratamiento de información personal, garantizando la autodeterminación informativa y la protección de los derechos fundamentales frente al uso de tecnologías de información. En este sentido, la protección constitucional de los datos personales constituye una manifestación del Estado constitucional de derecho y un mecanismo de control del poder público.

En el contexto del uso de sistemas de vigilancia digital en el sector público, la Constitución Política del Perú establece el marco jurídico que regula la actuación estatal, garantizando que el tratamiento de datos personales respete los principios de legalidad, proporcionalidad y protección de la dignidad humana.

2.3.2. Ley N.º 29733 — *Ley de Protección de Datos Personales*

La Ley N.º 29733, Ley de Protección de Datos Personales, constituye el principal instrumento normativo que regula el tratamiento de datos personales en el ordenamiento jurídico peruano. Su finalidad es garantizar el derecho fundamental a la protección de los datos personales mediante la regulación de su tratamiento por entidades públicas y privadas, estableciendo principios, obligaciones y mecanismos de tutela frente al uso indebido de información personal.

Esta norma establece principios fundamentales como legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad y disposición de recurso, los cuales

orientan el tratamiento de datos personales y garantizan el respeto de los derechos fundamentales del titular. Asimismo, reconoce derechos como acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

La Ley N.º 29733 también regula la creación del Registro Nacional de Protección de Datos Personales y establece el régimen de infracciones y sanciones aplicables en caso de incumplimiento de la normativa. De esta manera, la ley establece un sistema integral de protección de datos personales orientado a garantizar el control del individuo sobre su información personal.

En el ámbito del sector público, esta norma resulta especialmente relevante debido a que establece obligaciones específicas para las entidades estatales en el tratamiento de datos personales, garantizando el respeto de los derechos fundamentales frente al uso de sistemas de información y tecnologías digitales.

2.3.3.Reglamento de la Ley de Protección de Datos Personales

El Reglamento de la Ley N.º 29733, aprobado mediante Decreto Supremo N.º 003-2013-JUS, desarrolla las disposiciones de la Ley de Protección de Datos Personales y establece procedimientos específicos para la aplicación de sus principios y obligaciones. Este reglamento regula aspectos relacionados con el tratamiento de datos personales, el consentimiento del titular, las medidas de seguridad y el ejercicio de los derechos de los titulares de los datos.

Asimismo, el reglamento establece disposiciones sobre el tratamiento de datos sensibles, la transferencia de datos personales, la inscripción de bancos de datos personales y las obligaciones de los responsables del tratamiento. Estas disposiciones buscan garantizar la protección efectiva de la información personal frente a su uso indebido.

El reglamento también regula el procedimiento administrativo sancionador aplicable en caso de vulneración de la normativa sobre protección de datos personales, estableciendo mecanismos de control y supervisión del tratamiento de información personal.

En el contexto del uso de sistemas de vigilancia digital y tratamiento masivo de datos en el sector público, el reglamento constituye un instrumento fundamental para

garantizar la protección de la información personal y la aplicación efectiva de los principios de protección de datos.

2.3.4. Normativa sobre gobierno digital

La normativa sobre gobierno digital en el Perú regula el uso de tecnologías de la información y comunicación en la gestión pública, con el objetivo de mejorar la eficiencia administrativa, la transparencia y la prestación de servicios públicos. Entre las principales normas destacan el Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital, y las disposiciones relacionadas con la transformación digital del Estado.

Estas normas establecen principios como interoperabilidad, seguridad digital, protección de datos personales y acceso a la información pública, orientados a garantizar el uso adecuado de tecnologías digitales en la administración pública. Asimismo, regulan el uso de plataformas digitales, sistemas de identificación electrónica y mecanismos de intercambio de información entre entidades públicas.

El proceso de gobierno digital implica el tratamiento masivo de datos personales y el uso de sistemas tecnológicos en la gestión pública, lo que genera la necesidad de establecer mecanismos jurídicos que garanticen la protección de los derechos fundamentales en el entorno digital.

En este sentido, la normativa sobre gobierno digital debe interpretarse de manera coherente con la Constitución y la Ley de Protección de Datos Personales, garantizando el respeto de la privacidad y la protección de la información personal en la actuación estatal.

2.3.5. Jurisprudencia del Tribunal Constitucional

La jurisprudencia del Tribunal Constitucional peruano constituye una fuente fundamental para la interpretación y aplicación de los derechos fundamentales relacionados con la privacidad, la intimidad y la protección de datos personales. A través de sus pronunciamientos, el Tribunal ha desarrollado criterios sobre el alcance del derecho a la autodeterminación informativa y los límites del tratamiento de información personal por parte del Estado.

El Tribunal Constitucional ha señalado que el derecho a la protección de datos personales garantiza el control del individuo sobre su información personal y constituye un límite al ejercicio del poder estatal en el tratamiento de datos. Asimismo, ha establecido que cualquier intervención en la esfera privada debe cumplir con los principios de legalidad, necesidad y proporcionalidad.

La jurisprudencia constitucional también ha reconocido la importancia del proceso de hábeas data como mecanismo de tutela del derecho a la protección de datos personales, garantizando el acceso, rectificación y control de la información personal.

En el contexto del uso de sistemas de vigilancia digital por parte del Estado, la jurisprudencia del Tribunal Constitucional resulta relevante para establecer criterios interpretativos que permitan garantizar el respeto de los derechos fundamentales y la protección de la dignidad humana frente al tratamiento de información personal.

2.4.Marco conceptual

2.4.1.Derecho fundamental

El derecho fundamental es el conjunto de prerrogativas inherentes a la persona humana que gozan de reconocimiento constitucional y protección jurídica reforzada, orientadas a garantizar la dignidad humana, la libertad y la igualdad dentro del Estado constitucional de derecho. Estos derechos constituyen límites al ejercicio del poder estatal y garantizan las condiciones esenciales para el libre desarrollo de la personalidad y la convivencia democrática.

2.4.2.Protección de datos personales

La protección de datos personales es el derecho fundamental que garantiza a toda persona el control sobre la recopilación, almacenamiento, uso y difusión de su información personal, con el fin de evitar su tratamiento indebido o arbitrario. Este derecho busca proteger la privacidad, la dignidad humana y la autodeterminación informativa frente al uso de tecnologías de información por parte del Estado o de terceros.

2.4.3.Datos personales

Los datos personales son toda información que identifica o hace identificable a una persona natural, directa o indirectamente, mediante elementos como nombre, documento de identidad, características físicas, información económica, ubicación o datos biométricos. Estos datos constituyen el objeto de protección del derecho fundamental a la protección de datos personales.

2.4.4.Vigilancia digital

La vigilancia digital es el conjunto de prácticas y tecnologías destinadas a monitorear, registrar y analizar información sobre las personas mediante sistemas electrónicos, redes informáticas y dispositivos tecnológicos, con fines de control, seguridad o gestión administrativa. Esta práctica puede implicar el tratamiento masivo de información personal y generar implicancias jurídicas en la protección de los derechos fundamentales.

2.4.5.Intimidad

La intimidad es el derecho fundamental que protege el ámbito más reservado de la vida personal y familiar del individuo frente a injerencias arbitrarias del Estado o de terceros, garantizando un espacio de autonomía personal y el respeto de la dignidad humana. Este derecho comprende aspectos relacionados con la vida privada, las comunicaciones personales y las relaciones familiares.

2.4.6.Privacidad

La privacidad es el derecho que protege la esfera personal del individuo y su información frente a intromisiones indebidas, permitiendo el control sobre los datos relacionados con su vida personal, social y familiar. Este derecho garantiza la autonomía individual y el libre desarrollo de la personalidad en la sociedad contemporánea.

2.4.7.Autodeterminación informativa

La autodeterminación informativa es el principio jurídico que reconoce la facultad del individuo de controlar la recopilación, uso y difusión de su información personal, permitiéndole decidir sobre el tratamiento de los datos que le conciernen. Este principio

constituye la base del derecho a la protección de datos personales y garantiza la autonomía del individuo frente al tratamiento de información.

2.4.8.Sector público

El sector público comprende el conjunto de entidades, órganos e instituciones del Estado encargados de la administración de los recursos públicos y la prestación de servicios a la ciudadanía, actuando en el ejercicio de funciones administrativas, legislativas o jurisdiccionales conforme al ordenamiento jurídico.

2.4.9.Tratamiento de datos personales

El tratamiento de datos personales es cualquier operación o conjunto de operaciones realizadas sobre datos personales, como su recopilación, registro, almacenamiento, organización, uso, transmisión o eliminación, realizada por entidades públicas o privadas en el ejercicio de sus funciones.

2.4.10.Seguridad de la información

La seguridad de la información es el conjunto de medidas técnicas, organizativas y legales destinadas a proteger los datos frente a accesos no autorizados, pérdida, alteración o uso indebido, garantizando la confidencialidad, integridad y disponibilidad de la información en los sistemas de información.

CAPÍTULO III: CATEGORÍAS

3.1. Categorías y subcategorías de análisis

En la presente investigación, debido a su enfoque cualitativo y naturaleza jurídico-dogmática, el análisis se desarrolla mediante categorías y subcategorías que permiten examinar de manera sistemática el derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. Estas categorías se derivan del problema de investigación, objetivos y marco teórico.

Categoría 1: Protección del derecho fundamental a los datos personales

La protección de los datos personales constituye una manifestación del derecho fundamental a la intimidad y a la autodeterminación informativa, reconocidos en la Constitución Política del Perú y desarrollados por la Ley N.º 29733, Ley de Protección de Datos Personales. Este derecho garantiza que toda persona pueda ejercer control sobre la recopilación, uso, almacenamiento y transferencia de su información personal, especialmente frente a actuaciones del Estado. En el contexto de la vigilancia digital, este derecho adquiere especial relevancia debido al incremento del tratamiento masivo de datos por parte de entidades públicas.

Subcategorías

a) Protección constitucional de datos personales: Se refiere al reconocimiento normativo de los datos personales como parte del ámbito de protección de derechos fundamentales, particularmente la privacidad, la intimidad y la dignidad humana. La Constitución peruana reconoce estas garantías como límites al poder estatal.

b) Autodeterminación informativa: Es la facultad de toda persona para decidir sobre el uso y destino de su información personal. Este principio otorga al titular la capacidad de controlar quién accede a sus datos y con qué finalidad son tratados.

c) Principios del tratamiento de datos personales: Comprende los principios rectores que regulan el tratamiento de datos, como legalidad, consentimiento, finalidad, proporcionalidad, seguridad y calidad de los datos. Estos principios orientan la actuación legítima de las entidades públicas.

d) Derechos del titular de datos personales (ARCO): Son los derechos de acceso, rectificación, cancelación y oposición, que permiten al titular ejercer control efectivo sobre su información personal y exigir protección frente a usos indebidos.

Categoría 2: Sistemas de vigilancia digital en el sector público

Los sistemas de vigilancia digital son herramientas tecnológicas utilizadas por entidades públicas para monitorear, registrar y analizar información de ciudadanos con fines de seguridad, control administrativo o prestación de servicios públicos. Estas tecnologías incluyen cámaras de videovigilancia, reconocimiento facial, geolocalización, bases de datos interconectadas y plataformas digitales de monitoreo. Su implementación genera tensiones entre la seguridad pública y la protección de derechos fundamentales.

Subcategorías

a) Concepto de vigilancia digital: Hace referencia al conjunto de mecanismos tecnológicos que permiten la observación, recopilación y análisis automatizado de información personal en entornos físicos o digitales.

b) Tipos de sistemas de vigilancia digital: Incluye herramientas como videovigilancia, biometría, reconocimiento facial, monitoreo de redes, geolocalización y sistemas de inteligencia artificial aplicados a la gestión pública.

c) Vigilancia estatal y seguridad pública: Analiza la justificación del uso de sistemas de vigilancia como instrumento de prevención del delito, control del orden público y fortalecimiento de la seguridad ciudadana.

d) Tratamiento de datos en la administración pública: Examina cómo las entidades estatales recopilan, almacenan, comparten y utilizan datos personales dentro de procedimientos administrativos y políticas públicas.

Categoría 3: Límites jurídicos y vacíos normativos en el tratamiento de datos personales

El tratamiento de datos personales por parte del Estado debe sujetarse a límites jurídicos que garanticen el respeto de derechos fundamentales. Sin embargo, la rápida evolución de las tecnologías de vigilancia digital ha evidenciado vacíos regulatorios y desafíos

normativos que dificultan una protección efectiva de los datos personales. Esta categoría busca identificar tales limitaciones y analizar la suficiencia del marco jurídico vigente.

Subcategorías

a) Principio de legalidad: Establece que toda intervención estatal sobre datos personales debe estar previamente autorizada y regulada por ley, evitando actuaciones arbitrarias.

b) Principio de proporcionalidad: Exige que el tratamiento de datos sea idóneo, necesario y equilibrado respecto a la finalidad pública perseguida, evitando excesos en la vigilancia.

c) Límites del poder estatal: Se refiere a las restricciones constitucionales y legales que impiden al Estado invadir injustificadamente la esfera privada de las personas.

d) Deficiencias regulatorias: Comprende las insuficiencias normativas existentes en la legislación peruana respecto al uso de tecnologías emergentes de vigilancia digital.

e) Insuficiencia normativa frente a vigilancia digital: Analiza la falta de regulación específica sobre almacenamiento, acceso, conservación y eliminación de datos obtenidos mediante sistemas de vigilancia tecnológica.

3.2. Cuadro de categorización

Categorías	Subcategorías	Dimensiones
Protección del derecho fundamental a los datos personales	Protección constitucional de datos personales	Reconocimiento constitucional del derecho a la privacidad y protección de datos
	Autodeterminación informativa	Control del titular sobre la recopilación, uso y difusión de datos personales
	Principios del tratamiento de datos personales	Legalidad, consentimiento, finalidad, proporcionalidad y seguridad
	Derechos del titular de datos personales (ARCO)	Acceso, rectificación, cancelación y oposición

Sistemas de vigilancia digital en el sector público	Concepto de vigilancia digital	Naturaleza jurídica y tecnológica de la vigilancia digital
	Tipos de sistemas de vigilancia digital	Videovigilancia, biometría, reconocimiento facial, geolocalización
	Vigilancia estatal y seguridad pública	Finalidad preventiva, control social y seguridad ciudadana
	Tratamiento de datos en la administración pública	Recolección, almacenamiento, procesamiento y transferencia de datos
Límites jurídicos y vacíos normativos en el tratamiento de datos personales	Principio de legalidad	Base normativa y autorización legal del tratamiento de datos
	Principio de proporcionalidad	Idoneidad, necesidad y ponderación en la intervención estatal
	Límites del poder estatal	Restricciones constitucionales al ejercicio de vigilancia pública
	Deficiencias regulatorias	Ausencia de regulación específica sobre tecnologías emergentes
	Insuficiencia normativa frente a vigilancia digital	Protección limitada frente a nuevas formas de monitoreo digital

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Enfoque de investigación

La presente investigación adopta un enfoque cualitativo, orientado al análisis jurídico-dogmático del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. Según Roberto Hernández Sampieri, el enfoque cualitativo permite comprender fenómenos a partir de la interpretación de realidades complejas dentro de su contexto natural, privilegiando el análisis profundo sobre la medición numérica. En ese sentido, este enfoque resulta pertinente porque posibilita examinar el fenómeno de estudio mediante la interpretación sistemática de normas constitucionales, legales, doctrina y jurisprudencia, con el propósito de comprender el alcance de la protección jurídica de los datos personales, identificar los límites del tratamiento de información por parte del Estado y analizar los vacíos del marco normativo vigente.

4.2. Nivel de investigación

El estudio corresponde a un nivel descriptivo–analítico. Conforme señala Mario Tamayo y Tamayo, la investigación descriptiva busca identificar, caracterizar y detallar las propiedades esenciales de un fenómeno, mientras que el nivel analítico permite descomponer sus elementos para examinar su naturaleza y relaciones jurídicas. En ese marco, la presente investigación es descriptiva porque busca identificar y explicar el marco jurídico que regula la protección de datos personales frente al uso de sistemas de vigilancia digital; y es analítica porque examina críticamente las normas, principios y mecanismos jurídicos aplicables, evaluando sus alcances, limitaciones y efectos en la protección de los derechos fundamentales.

4.3. Tipo de investigación

La investigación es de tipo básica o pura. Según César Bernal, la investigación básica tiene como finalidad ampliar y profundizar el conocimiento científico sin buscar una aplicación práctica inmediata. En ese sentido, este estudio se orienta a ampliar el conocimiento teórico y jurídico sobre la protección del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. Su finalidad es generar conocimiento doctrinario y jurídico que contribuya al desarrollo del

derecho constitucional y del derecho administrativo en materia de protección de datos personales.

4.4.Método de la Investigación

La investigación emplea principalmente el método jurídico-dogmático, orientado al estudio sistemático del ordenamiento jurídico mediante el análisis, interpretación e integración de normas legales, constitucionales y jurisprudenciales relacionadas con la protección de datos personales. Asimismo, se emplea el método hermenéutico jurídico para interpretar el contenido y alcance de las normas jurídicas, y el método analítico–sintético para examinar los elementos del fenómeno investigado y formular conclusiones jurídicas sobre la tutela del derecho a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público.

4.5.Diseño de la investigación

La investigación presenta un diseño no experimental de carácter documental y transversal. De acuerdo con Roberto Hernández Sampieri, un diseño no experimental se caracteriza por observar los fenómenos tal como ocurren en su contexto natural, sin manipulación de variables. En ese sentido, es no experimental porque no se realizan intervenciones sobre el objeto de estudio, sino que se analizan normas jurídicas, doctrina y jurisprudencia existentes. Asimismo, es documental porque se basa en el análisis de fuentes jurídicas como legislación, jurisprudencia, doctrina y documentos especializados. Finalmente, es transversal porque el estudio se realiza en un determinado periodo temporal, permitiendo examinar el fenómeno jurídico en un momento específico sin seguimiento longitudinal.

4.6. Población y Muestra

4.6.1.Población

Está conformada por profesionales especializados en derecho constitucional, derecho administrativo, derecho digital, protección de datos personales y gestión pública, tales como abogados, jueces, fiscales, funcionarios públicos, especialistas en gobierno digital y académicos con conocimiento en la materia objeto de estudio.

4.6.2. Muestra

La muestra de informantes está conformada por especialistas seleccionados mediante muestreo no probabilístico por criterio o intencional, considerando su experiencia profesional y conocimiento en materia de protección de datos personales, derechos fundamentales o administración pública, siendo **10 expertos**, entre ellos:

- Abogados especialistas en derecho constitucional o digital.
- Funcionarios del sector público vinculados al tratamiento de datos.
- Docentes universitarios en Derecho.
- Especialistas en gobierno digital o protección de datos personales.

4.7. Técnicas en instrumentos de recojo de la información

En la presente investigación se emplean técnicas de recolección de información acordes con el enfoque cualitativo y el método jurídico-dogmático, orientadas a obtener información relevante para el análisis del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. Las técnicas utilizadas son el análisis documental y la entrevista, las cuales permiten recopilar información doctrinaria, normativa y empírica relevante para el desarrollo del estudio.

4.7.1. Técnicas de recojo de información

a) Análisis documental

El análisis documental consiste en la revisión sistemática e interpretación de normas jurídicas, doctrina especializada, jurisprudencia y documentos relacionados con el derecho a la protección de datos personales y el uso de sistemas de vigilancia digital en el sector público. Esta técnica permite examinar el marco normativo, doctrinario y jurisprudencial aplicable al objeto de estudio, facilitando la comprensión del fenómeno investigado desde una perspectiva jurídica.

b) Entrevista

La entrevista es una técnica cualitativa que permite obtener información directa de especialistas con conocimiento en materia de protección de datos personales, derechos

fundamentales y gestión pública. Se aplicarán entrevistas semiestructuradas a expertos, con la finalidad de conocer sus opiniones, experiencias y criterios jurídicos respecto a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano.

4.7.2. Instrumentos de recojo de información

a) Ficha de análisis documental

La ficha de análisis documental es el instrumento utilizado para registrar, organizar y sistematizar la información obtenida de las fuentes normativas, doctrinarias y jurisprudenciales. Este instrumento permite identificar el contenido relevante de los documentos analizados, facilitando su interpretación y posterior análisis jurídico.

b) Guía de entrevista

La guía de entrevista es el instrumento que contiene un conjunto de preguntas previamente elaboradas en función de las categorías y subcategorías de investigación. Este instrumento permite orientar la recolección de información de los especialistas entrevistados, garantizando la coherencia y pertinencia de las respuestas respecto al objeto de estudio.

4.8. Aspectos éticos

La presente investigación se desarrolla respetando los principios éticos fundamentales que rigen la actividad científica, garantizando la integridad académica, la veracidad de la información y el respeto de los derechos de las personas participantes en el estudio.

En primer lugar, se respeta el principio de honestidad académica, asegurando el uso adecuado de fuentes bibliográficas, normativas y doctrinarias, mediante la correcta citación y referencia de los autores consultados conforme a las normas APA, evitando cualquier forma de plagio o apropiación indebida de información.

Asimismo, en la aplicación de entrevistas a los especialistas participantes se garantiza el respeto del principio de consentimiento informado, informando previamente a los entrevistados sobre los objetivos de la investigación.

CAPÍTULO V: PRESENTACIÓN DE RESULTADOS

El presente capítulo tiene como finalidad exponer, analizar e interpretar los resultados obtenidos en el desarrollo de la investigación, en concordancia con los objetivos planteados y el enfoque metodológico adoptado. Para ello, se emplearon técnicas de recolección de datos como el análisis documental y la entrevista a especialistas, lo que permitió obtener información relevante respecto a la protección del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano.

Los resultados se presentan de manera organizada a través de categorías y subcategorías previamente definidas, las cuales responden a las variables de estudio. En este sentido, se abordan aspectos vinculados a la protección del derecho a los datos personales, la implementación de sistemas de vigilancia digital en el sector público, los límites jurídicos del tratamiento de datos personales y los vacíos existentes en el marco normativo.

Asimismo, el análisis no se limita a una descripción de los hallazgos, sino que incorpora una interpretación crítica de los mismos, estableciendo su relación con el marco teórico y los antecedentes de investigación. De esta manera, se busca evidenciar las coincidencias, divergencias y aportes relevantes que permitan comprender la problemática desde una perspectiva integral.

5.1.Resultados de la ficha documental

Tabla 1 Ficha de análisis documental N.º F-01

Documento	Tipo	Nivel de protección
Ley N.º 29733	Norma	Moderado
Hallazgo principal	El Reglamento de la Ley N.º 29733 desarrolla los principios y disposiciones aplicables al tratamiento de datos personales, precisando condiciones para el consentimiento, el deber de información, las medidas de seguridad, el registro de bancos de datos y las competencias de la Autoridad Nacional de Protección de Datos Personales. Asimismo, regula las obligaciones de las	

	entidades públicas en el tratamiento de datos, estableciendo criterios para garantizar la legalidad y seguridad de la información.
Vacíos o limitaciones	No regula de forma específica los sistemas de vigilancia digital ni tecnologías emergentes.
Límites jurídicos identificados	Consentimiento, finalidad, proporcionalidad, legalidad.
Observaciones	Se identifica una falta de regulación específica sobre vigilancia digital en el sector público , especialmente en relación con tecnologías avanzadas como el reconocimiento facial o el monitoreo automatizado. Asimismo, se advierte una limitada precisión en los mecanismos de fiscalización y control frente al uso indebido de datos personales por parte de entidades estatales.

El análisis del contenido de la Ley N.º 29733 evidencia que el ordenamiento jurídico peruano ha desarrollado un marco normativo relevante para la protección del derecho fundamental a los datos personales, estableciendo principios rectores como el consentimiento, la finalidad, la proporcionalidad y la legalidad en el tratamiento de la información. En concordancia con el marco teórico, estos principios constituyen manifestaciones concretas del derecho a la autodeterminación informativa y operan como límites al ejercicio del poder estatal en el tratamiento de datos personales.

No obstante, desde una perspectiva crítica, se advierte que dicha normativa presenta insuficiencias frente a los avances tecnológicos contemporáneos, particularmente en relación con los sistemas de vigilancia digital en el sector público. Tal como lo sostienen los antecedentes revisados —especialmente Acevedo Paredes y Paredes Torres (2024) y Mejía Arbildo (2023)—, el desarrollo de tecnologías como la inteligencia artificial y el tratamiento automatizado de datos ha superado la capacidad regulativa de la legislación vigente, generando vacíos normativos que debilitan la protección efectiva de los derechos fundamentales.

En este mismo sentido, el hallazgo de la tabla resulta coherente con la base teórica sobre sistemas de vigilancia digital, en la medida en que estos implican una recopilación

masiva, automatizada y potencialmente invasiva de datos personales, lo cual exige estándares más estrictos de control jurídico. Sin embargo, la Ley N.º 29733 no regula de manera específica herramientas como el reconocimiento facial o el monitoreo automatizado, lo que evidencia una desactualización normativa frente a la transformación digital del Estado.

Asimismo, si bien la norma establece competencias para la Autoridad Nacional de Protección de Datos Personales, se observa —como correctamente señala la ficha— una limitada precisión en los mecanismos de fiscalización y control, lo cual reduce la eficacia de la tutela jurídica. Este aspecto resulta especialmente crítico en el sector público, donde existe una relación asimétrica entre el Estado y el ciudadano, tal como lo desarrolla el marco teórico en el apartado de tratamiento de datos personales en la administración pública.

Por otro lado, los límites jurídicos identificados (consentimiento, finalidad, proporcionalidad y legalidad), aunque adecuados desde un enfoque dogmático, no resultan suficientes en contextos de vigilancia masiva, donde el consentimiento puede verse debilitado o incluso resultar inaplicable. Esta situación coincide con lo señalado por Haro Benites y Moncada Hernández (2024), quienes advierten que la vigilancia estatal puede vulnerar derechos fundamentales si no se establecen controles estrictos y garantías constitucionales reforzadas.

Tabla 2 Ficha de análisis documental N.º F-02

Documento	Tipo	Nivel de protección
D.S. N.º 003-2013-JUS – Reglamento de la Ley de Protección de Datos Personales	Norma	Moderado
Hallazgo principal	El reglamento fortalece el marco normativo al desarrollar de manera más precisa los principios de la ley, especialmente en lo referido al consentimiento, seguridad de los datos y obligaciones de las entidades públicas. No obstante, mantiene un enfoque general y no regula de manera específica el uso de sistemas de vigilancia digital, como	

	cámaras inteligentes o reconocimiento facial, lo que limita su eficacia frente a tecnologías emergentes.
Vacíos o limitaciones	No contempla regulación específica sobre vigilancia digital ni mecanismos de control en contextos de monitoreo estatal.
Límites jurídicos identificados	Consentimiento informado, deber de información, medidas de seguridad.
Observaciones	Se identifica una falta de regulación específica sobre vigilancia digital en el sector público, especialmente en relación con tecnologías avanzadas como el reconocimiento facial o el monitoreo automatizado. Asimismo, se advierte una limitada precisión en los mecanismos de fiscalización y control frente al uso indebido de datos personales por parte de entidades estatales.

El Reglamento de la Ley N.º 29733 (D.S. N.º 003-2013-JUS) desarrolla de manera más detallada los principios del tratamiento de datos personales, especialmente en lo relativo al consentimiento informado, el deber de información y las medidas de seguridad, reforzando así la tutela del derecho a la protección de datos personales en el ordenamiento peruano. En concordancia con el marco teórico, estos elementos constituyen garantías esenciales de la autodeterminación informativa y límites al ejercicio del poder estatal.

Sin embargo, desde una perspectiva crítica y en línea con los antecedentes de investigación, se advierte que el reglamento mantiene un enfoque general que resulta insuficiente frente a los avances tecnológicos. En particular, no regula de manera específica el uso de sistemas de vigilancia digital en el sector público, como el reconocimiento facial o el monitoreo automatizado, lo que evidencia un vacío normativo relevante frente al tratamiento masivo y automatizado de datos personales.

Asimismo, aunque se establecen obligaciones para las entidades públicas, se observa una limitada precisión en los mecanismos de fiscalización y control, lo que debilita la eficacia de la protección jurídica. En consecuencia, se confirma la existencia de una brecha entre la regulación vigente y las nuevas formas de vigilancia digital, lo cual

incide directamente en la necesidad de reforzar los límites jurídicos y garantizar una tutela más efectiva de los derechos fundamentales frente al uso de tecnologías emergentes.

Tabla 3 Ficha de análisis documental N.º F-03

Documento	Tipo	Nivel de protección
Exp. N.º 1797-2002-HD/TC	Jurisprudencia	Alto
Hallazgo principal	El derecho a la autodeterminación informativa garantiza a toda persona el control sobre la información que le concierne, limitando el poder del Estado en el tratamiento de datos personales.	
Vacíos o limitaciones	No aborda tecnologías modernas	
Límites jurídicos identificados	Proporcionalidad, legalidad, control del titular	
Observaciones	Se advierte que, si bien existe un sólido reconocimiento constitucional del derecho , la jurisprudencia no ha evolucionado al mismo ritmo que las tecnologías de vigilancia digital, lo que genera desafíos en su aplicación práctica en el sector público.	

La jurisprudencia contenida en el Exp. N.º 1797-2002-HD/TC constituye un referente fundamental en el reconocimiento del derecho a la autodeterminación informativa como manifestación del derecho a la protección de datos personales, al establecer que toda persona tiene control sobre la información que le concierne. En concordancia con el marco teórico, este criterio delimita el ejercicio del poder estatal mediante principios como legalidad y proporcionalidad, consolidando un alto nivel de protección constitucional.

No obstante, desde una perspectiva crítica y en relación con los antecedentes analizados, se advierte que dicha jurisprudencia no incorpora los desafíos derivados del uso de tecnologías modernas de vigilancia digital. En efecto, la ausencia de criterios específicos sobre tratamiento automatizado de datos, reconocimiento facial o monitoreo masivo limita su aplicabilidad en contextos actuales, especialmente en el sector público.

En consecuencia, si bien existe un sólido desarrollo constitucional del derecho, se evidencia una falta de actualización jurisprudencial frente a la transformación digital, lo que genera una brecha entre la interpretación constitucional y las nuevas formas de tratamiento de datos personales, afectando la eficacia de su tutela en la práctica.

Tabla 4 Ficha de análisis documental N.º F-04

Documento	Tipo	Nivel de protección
Derecho y Razón. Teoría del garantismo penal	Doctrina	Limitado
Hallazgo principal	El poder del Estado debe estar limitado por garantías jurídicas que aseguren la protección efectiva de los derechos fundamentales y eviten cualquier forma de arbitrariedad.	
Vacíos o limitaciones	No aborda tecnologías modernas	
Límites jurídicos identificados	Legalidad, proporcionalidad, control estatal	
Observaciones	Se advierte que el principal problema no radica únicamente en la existencia de normas, sino en su efectiva implementación y control, lo que evidencia una brecha entre el reconocimiento formal del derecho y su protección material en la realidad.	

La obra Derecho y Razón. Teoría del garantismo penal aporta un fundamento doctrinario esencial al establecer que el ejercicio del poder estatal debe estar estrictamente limitado por garantías jurídicas orientadas a la protección de los derechos fundamentales. En concordancia con el marco teórico, principios como la legalidad y la proporcionalidad se configuran como límites indispensables frente a posibles arbitrariedades, siendo plenamente aplicables al tratamiento de datos personales y al uso de sistemas de vigilancia por parte del Estado.

No obstante, desde una perspectiva crítica, se advierte que esta teoría no aborda de manera específica los desafíos derivados del desarrollo de tecnologías modernas, como los sistemas de vigilancia digital o el tratamiento automatizado de datos personales. En

línea con los antecedentes analizados, esta limitación evidencia la necesidad de reinterpretar los postulados del garantismo en el contexto de la transformación digital.

En consecuencia, se confirma que el problema no radica únicamente en la existencia de un marco normativo o doctrinario adecuado, sino en su efectiva implementación y control. Ello revela una brecha entre el reconocimiento formal de los derechos fundamentales y su protección material en la práctica, especialmente en el ámbito del sector público frente al uso de tecnologías de vigilancia digital.

Tabla 5 Ficha de análisis documental N.º F-05

Documento	Tipo	Nivel de protección
Defensoría del Pueblo	Informe	Limitado
Hallazgo principal	Las entidades públicas presentan debilidades en la implementación de la normativa sobre protección de datos personales, lo que incrementa el riesgo de vulneración de derechos fundamentales en contextos de uso de tecnologías digitales.	
Vacíos o limitaciones	Falta de implementación y regulación digital	
Límites jurídicos identificados	Control, seguridad, supervisión	
Observaciones	Se identifica una débil cultura de protección de datos en el sector público, así como la ausencia de mecanismos eficaces de supervisión y sanción. Asimismo, se advierte la necesidad de actualizar el marco normativo frente al avance de tecnologías digitales.	

El informe de la Defensoría del Pueblo evidencia que, pese a la existencia de un marco normativo sobre protección de datos personales, las entidades públicas presentan debilidades significativas en su implementación, lo que incrementa el riesgo de vulneración de derechos fundamentales. En concordancia con el marco teórico, esta

situación refleja una insuficiente materialización de principios como seguridad, control y supervisión en el tratamiento de datos personales.

Desde una perspectiva crítica y en línea con los antecedentes analizados, se advierte que el problema no se limita a vacíos normativos, sino que se extiende a una deficiente cultura institucional de protección de datos en el sector público. La ausencia de mecanismos eficaces de fiscalización y sanción debilita la tutela jurídica del derecho, especialmente en contextos de uso de tecnologías digitales y sistemas de vigilancia.

En consecuencia, se confirma la existencia de una brecha entre el reconocimiento formal del derecho y su aplicación efectiva, lo que evidencia la necesidad de fortalecer tanto la regulación como los mecanismos de supervisión y control, a fin de garantizar una protección real y adecuada de los datos personales frente a los desafíos de la transformación digital.

Tabla 6 Ficha de análisis documental N.º F-06

Documento	Tipo	Nivel de protección
Unión Europea	Internacional	Alto
Hallazgo principal	El tratamiento de datos personales debe ser lícito, transparente y limitado a fines específicos, garantizando la protección efectiva de los derechos del titular mediante mecanismos de control y supervisión.	
Vacíos o limitaciones	No aplicable directamente en Perú	
Límites jurídicos identificados	Minimización, transparencia, evaluación de impacto	
Observaciones	El RGPD evidencia la necesidad de que el ordenamiento peruano actualice su marco normativo, incorporando regulaciones específicas sobre vigilancia digital, mecanismos de evaluación de impacto y fortalecimiento de la supervisión institucional.	

El modelo de la Unión Europea, particularmente a través del Reglamento General de Protección de Datos (RGPD), establece estándares avanzados en materia de protección de datos personales, basados en principios como licitud, transparencia y limitación de la finalidad. En concordancia con el marco teórico, estos principios refuerzan la autodeterminación informativa y consolidan mecanismos eficaces de control y supervisión en el tratamiento de datos personales.

Desde una perspectiva crítica y conforme a los antecedentes analizados, este modelo evidencia las limitaciones del ordenamiento peruano, el cual aún mantiene un enfoque general y menos desarrollado frente a los desafíos de la vigilancia digital. En particular, la ausencia de instrumentos como la evaluación de impacto en protección de datos y la regulación específica de tecnologías emergentes refleja una brecha normativa significativa.

En consecuencia, si bien el RGPD no resulta directamente aplicable en el Perú, constituye un referente relevante que pone de manifiesto la necesidad de actualizar el marco normativo nacional, incorporando estándares más rigurosos de protección, supervisión institucional y regulación específica frente al uso de sistemas de vigilancia digital en el sector público.

5.2.Resultados de las entrevistas

Tabla 7 Categoría 1: Protección del derecho fundamental a los datos personales

Subcategoría	Hallazgo principal	Evidencia (Entrevistados)	Interpretación
Regulación normativa	El derecho está reconocido en la Constitución y en la ley	E-01, E-02, E-04, E-08, E-09	Se observa que el ordenamiento jurídico peruano sí reconoce este derecho; sin embargo, su desarrollo aún no es suficiente frente a la realidad digital actual
Eficacia normativa	La normativa no garantiza	E-01, E-03, E-04, E-10	Esto permite advertir que la norma existe,

	plenamente la protección		pero no logra proteger de manera efectiva en todos los casos, especialmente frente a nuevas tecnologías
Aplicación práctica	Deficiencias en la implementación en entidades públicas	E-05, E-06, E-07	Se evidencia que el problema no solo es normativo, sino también práctico, debido a fallas en la gestión pública
Desfase tecnológico	La normativa está desactualizada	E-03, E-06, E-09	Se puede inferir que el derecho no ha evolucionado al mismo ritmo que la tecnología
Autodeterminación informativa	Es un principio clave pero poco aplicado	E-01, E-04, E-08, E-10	Aunque es un principio importante, en la práctica el ciudadano no siempre tiene control real sobre sus datos

El análisis de la Categoría 1 evidencia que el ordenamiento jurídico peruano reconoce formalmente el derecho fundamental a la protección de datos personales, tanto a nivel constitucional como legal, lo cual resulta coherente con el marco teórico desarrollado. No obstante, en concordancia con los antecedentes de investigación, este reconocimiento presenta limitaciones en su desarrollo normativo, especialmente frente a los desafíos de la transformación digital.

Desde una perspectiva crítica, se advierte que la eficacia normativa es limitada, ya que la existencia de la norma no garantiza una protección efectiva en la práctica, particularmente frente al uso de tecnologías emergentes y sistemas de vigilancia digital. Asimismo, los resultados evidencian deficiencias en la aplicación práctica dentro de las entidades públicas, lo que confirma que el problema no es únicamente normativo, sino también institucional y operativo.

Por otro lado, se identifica un desfase entre la evolución tecnológica y la actualización del marco jurídico, lo cual debilita la tutela del derecho en contextos digitales. En este escenario, si bien la autodeterminación informativa constituye un principio esencial, su aplicación resulta aún incipiente, limitando el control real del ciudadano sobre sus datos personales.

En consecuencia, se confirma la existencia de una brecha entre el reconocimiento formal del derecho y su protección efectiva, lo que evidencia la necesidad de fortalecer tanto la regulación como su implementación, a fin de garantizar una tutela adecuada frente a los retos de la vigilancia digital en el sector público.

Tabla 8 Categoría 2: Sistemas de vigilancia digital en el sector público

Subcategoría	Hallazgo principal	Evidencia	Interpretación
Implementación estatal	Uso creciente de sistemas de vigilancia	E-05, E-06, E-07	Se observa que el Estado viene utilizando cada vez más estas tecnologías, principalmente por razones de seguridad
Falta de regulación	No existe regulación específica	E-01, E-03, E-09	Esto demuestra que el uso de estas herramientas no está completamente regulado, lo que genera inseguridad jurídica
Riesgos identificados	Vigilancia masiva, uso indebido de datos	E-01, E-03, E-05, E-09	Se advierte que estos sistemas pueden afectar derechos fundamentales si no se controlan adecuadamente
Seguridad vs derechos	No hay equilibrio adecuado	E-02, E-04, E-08	Se puede apreciar que muchas veces se prioriza la seguridad sobre los derechos fundamentales
Control institucional	Débil supervisión estatal	E-06, E-07, E-10	Esto evidencia que el Estado no cuenta con mecanismos

			suficientes para controlar el uso de estos sistemas
Problemas operativos	Implementación desordenada	E-05, E-06	Se observa una falta de planificación y organización en el uso de estas tecnologías

El análisis de la Categoría 2 evidencia un uso creciente de sistemas de vigilancia digital por parte del Estado, principalmente justificado en razones de seguridad pública, lo cual resulta coherente con el marco teórico sobre vigilancia estatal. No obstante, en concordancia con los antecedentes, este incremento no ha sido acompañado por un desarrollo normativo específico, generando un escenario de inseguridad jurídica en el tratamiento de datos personales.

Desde una perspectiva crítica, se advierte que la ausencia de regulación específica sobre estas tecnologías permite la existencia de riesgos significativos, tales como la vigilancia masiva y el uso indebido de datos personales, lo que puede derivar en vulneraciones a derechos fundamentales como la privacidad y la autodeterminación informativa. Asimismo, se evidencia una falta de equilibrio entre la seguridad pública y la protección de derechos, donde en la práctica suele prevalecer el interés estatal sobre las garantías individuales.

Por otro lado, los resultados muestran una débil capacidad de control institucional, caracterizada por la ausencia de mecanismos eficaces de supervisión, así como problemas operativos en la implementación de estos sistemas, reflejados en una gestión desordenada y carente de planificación. En consecuencia, se confirma que el uso de sistemas de vigilancia digital en el sector público peruano presenta deficiencias tanto normativas como institucionales, lo que refuerza la necesidad de establecer límites jurídicos claros y mecanismos de control efectivos para garantizar la protección de los derechos fundamentales.

Tabla 9 Categoría 3: Límites jurídicos del tratamiento de datos personales

Subcategoría	Hallazgo principal	Evidencia	Interpretación
Principios jurídicos	Legalidad, proporcionalidad, finalidad	E-01, E-02, E-04, E-09	Se reconoce que existen principios jurídicos claros que deberían limitar el uso de datos personales
Límites constitucionales	Necesidad y control judicial	E-04, E-08	Se puede señalar que estos límites son importantes, pero no siempre se aplican en la práctica
Límites técnicos	Seguridad y control de acceso	E-06, E-10	Se observa que el aspecto técnico es clave, pero aún no está bien desarrollado en el sector público
Mecanismos de control	Son insuficientes	E-02, E-05, E-06, E-07	Se evidencia que el control existente no es suficiente para garantizar la protección del derecho
Fiscalización estatal	Supervisión limitada	E-05, E-06	Esto refleja una debilidad institucional en el control del tratamiento de datos
Responsabilidad del Estado	Falta claridad	E-02, E-03	Se puede advertir que no está bien definido quién responde ante vulneraciones

El análisis de la Categoría 3 evidencia que el ordenamiento jurídico reconoce principios fundamentales —como legalidad, proporcionalidad y finalidad— que deben limitar el tratamiento de datos personales, en concordancia con el marco teórico. Asimismo, se identifican límites constitucionales relevantes, como la necesidad y el control judicial, los cuales constituyen garantías esenciales frente a posibles excesos del poder estatal.

No obstante, desde una perspectiva crítica y conforme a los antecedentes, se advierte que dichos límites no se aplican de manera efectiva en la práctica. En particular, los mecanismos de control resultan insuficientes y la fiscalización estatal es limitada, lo que debilita la tutela del derecho a la protección de datos personales, especialmente en contextos de vigilancia digital.

Por otro lado, se observa que los límites técnicos, como la seguridad y el control de acceso, aún no se encuentran adecuadamente desarrollados en el sector público, lo que incrementa el riesgo de uso indebido de la información. Asimismo, la falta de claridad en la determinación de la responsabilidad del Estado frente a vulneraciones evidencia un vacío relevante en el sistema de protección.

En consecuencia, se confirma que, si bien existen límites jurídicos formales, estos presentan deficiencias en su implementación y control, lo que evidencia la necesidad de fortalecer tanto los mecanismos institucionales como la regulación específica para garantizar una protección efectiva de los datos personales.

Tabla 10 Categoría 4: Vacíos del marco normativo

Subcategoría	Hallazgo principal	Evidencia	Interpretación
Vacíos legales	No hay regulación específica de vigilancia digital	E-01, E-03, E-09	Se identifica una ausencia normativa clara frente a estas tecnologías
Vacíos tecnológicos	Falta regulación de IA y DPIA	E-03, E-10	Se observa que la normativa no contempla herramientas modernas de tratamiento de datos
Vacíos institucionales	Deficiente implementación	E-05, E-07, E-08	Se puede inferir que las instituciones no están preparadas para aplicar la normativa
Vacíos operativos	Falta de protocolos	E-05, E-07	Esto evidencia problemas en la gestión interna de las entidades públicas

Falta de control	Supervisión débil	E-06, E-10	Se aprecia que el control estatal es limitado y poco efectivo
Propuestas de mejora	Necesidad de reformas	E-01 a E-10	De manera general, los entrevistados coinciden en que se requiere una mejora integral del sistema

El análisis de la Categoría 4 evidencia la existencia de vacíos significativos en el marco normativo peruano respecto a la protección de datos personales frente a sistemas de vigilancia digital. En concordancia con el marco teórico y los antecedentes, se identifica una ausencia de regulación específica sobre estas tecnologías, lo que genera inseguridad jurídica y limita la capacidad del ordenamiento para responder a los desafíos de la transformación digital.

Desde una perspectiva crítica, no solo se observan vacíos legales, sino también tecnológicos e institucionales. La normativa vigente no contempla herramientas modernas como la inteligencia artificial ni mecanismos preventivos como las evaluaciones de impacto en protección de datos, lo que refleja un desfase frente a los estándares internacionales. Asimismo, las entidades públicas presentan deficiencias en la implementación, evidenciando una limitada capacidad institucional para aplicar adecuadamente la normativa.

Por otro lado, se advierten vacíos operativos, como la ausencia de protocolos claros para el tratamiento de datos personales, así como una débil supervisión estatal, lo que afecta la eficacia de los mecanismos de control. En este contexto, la falta de articulación entre regulación, implementación y fiscalización debilita la tutela efectiva del derecho fundamental.

En consecuencia, los resultados permiten afirmar que los vacíos del marco normativo son estructurales y multidimensionales, lo que justifica la necesidad de una reforma integral que incorpore regulación específica sobre vigilancia digital, fortalezca los mecanismos de control institucional y adecúe el ordenamiento jurídico a las exigencias de la sociedad digital.

CAPÍTULO VI: DISCUSIÓN DE RESULTADOS

Los resultados obtenidos en la presente investigación evidencian que, si bien el ordenamiento jurídico peruano reconoce el derecho fundamental a la protección de datos personales a nivel constitucional y legal, su eficacia en contextos de vigilancia digital en el sector público resulta limitada. Este hallazgo coincide con lo desarrollado en el marco teórico, donde se establece que la autodeterminación informativa constituye un pilar esencial del Estado constitucional de derecho; sin embargo, en la práctica, su aplicación es aún incipiente.

En relación con los antecedentes, los resultados coinciden con lo señalado por Acevedo Paredes y Paredes Torres (2024) y Mejía Arbildo (2023), quienes sostienen que el avance tecnológico, especialmente en el uso de inteligencia artificial y tratamiento automatizado de datos, ha superado la capacidad regulativa del marco normativo vigente. En ese sentido, se evidenció un desfase entre la evolución tecnológica y la actualización del derecho, lo cual se refleja en la ausencia de regulación específica sobre sistemas de vigilancia digital, como el reconocimiento facial o el monitoreo automatizado.

Asimismo, los resultados demostraron que la existencia de normas como la Ley N.º 29733 y su reglamento no garantiza por sí sola la protección efectiva del derecho, lo cual coincide con lo señalado en el informe de la Defensoría del Pueblo. En efecto, se evidenció que las entidades públicas presentan deficiencias en la implementación de la normativa, así como una débil cultura institucional de protección de datos personales, lo que incrementa el riesgo de vulneraciones a derechos fundamentales.

Por otro lado, en cuanto a los límites jurídicos del tratamiento de datos personales, si bien se reconocen principios como legalidad, proporcionalidad y finalidad, se evidenció que estos no se aplican de manera efectiva en la práctica. Estos resultados coinciden con lo expuesto por Haro Benites y Moncada Hernández (2024), quienes advierten que la vigilancia estatal puede generar afectaciones a derechos fundamentales cuando no existen mecanismos de control adecuados. En este sentido, se identificó una limitada fiscalización estatal y una falta de claridad en la responsabilidad frente a posibles vulneraciones, lo que debilita la tutela jurídica del derecho.

Del mismo modo, los resultados evidenciaron que el uso creciente de sistemas de vigilancia digital en el sector público no ha sido acompañado por mecanismos adecuados

de regulación, supervisión y control. Esta situación genera una tensión entre la seguridad pública y la protección de los derechos fundamentales, donde, en la práctica, suele prevalecer el interés estatal. Este hallazgo guarda relación con el marco teórico sobre vigilancia digital, el cual advierte que el uso de estas tecnologías puede derivar en prácticas de vigilancia masiva si no se establecen límites jurídicos claros.

Finalmente, los resultados permitieron identificar la existencia de vacíos normativos, tecnológicos e institucionales en el ordenamiento peruano, lo cual coincide con estándares comparados como el modelo europeo (RGPD), que incorpora mecanismos más avanzados como la evaluación de impacto en protección de datos y mayores niveles de supervisión. En consecuencia, se evidenció la necesidad de una reforma integral que permita adecuar el marco normativo a los desafíos de la transformación digital, fortaleciendo la protección efectiva del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público.

6.1.Propuesta de incorporación normativa a la Ley N.º 29733

En atención a los resultados obtenidos, se propone la incorporación de un capítulo específico referido al uso de sistemas de vigilancia digital en el sector público, con el siguiente contenido:

- **Artículo X: Regulación de sistemas de vigilancia digital**

El uso de sistemas de vigilancia digital por parte de entidades públicas deberá sujetarse a los principios de legalidad, proporcionalidad, finalidad, necesidad y minimización de datos, garantizando en todo momento la protección de los derechos fundamentales de los ciudadanos.

- **Artículo X+1: Evaluación de impacto en protección de datos personales**

Las entidades públicas deberán realizar una evaluación de impacto en protección de datos personales de manera previa a la implementación de sistemas de vigilancia digital, a fin de identificar y mitigar riesgos para los derechos fundamentales.

- **Artículo X+2: Transparencia y deber de información**

Las entidades públicas deberán informar de manera clara, accesible y oportuna sobre la utilización de sistemas de vigilancia digital, incluyendo su finalidad, alcance y tiempo de almacenamiento de los datos.

- **Artículo X+3: Supervisión y control**

La Autoridad Nacional de Protección de Datos Personales deberá supervisar el uso de estos sistemas, pudiendo realizar auditorías y aplicar sanciones en caso de incumplimiento.

CONCLUSIONES

1. Se determinó que la protección jurídica del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano es formalmente reconocida pero materialmente insuficiente, debido a la existencia de vacíos normativos, debilidades institucionales y limitaciones en los mecanismos de control, lo que afecta su tutela efectiva en contextos de transformación digital.
2. Se estableció que los límites jurídicos del tratamiento de datos personales —como los principios de legalidad, proporcionalidad, finalidad y consentimiento— no se aplican de manera efectiva en la práctica, especialmente en escenarios de vigilancia digital, debido a la insuficiencia de mecanismos de fiscalización, la débil supervisión estatal y la falta de desarrollo de estándares técnicos adecuados.
3. Se identificó que el marco normativo peruano presenta vacíos significativos en la regulación de sistemas de vigilancia digital, particularmente en lo referido al uso de tecnologías emergentes como la inteligencia artificial, el reconocimiento facial y el tratamiento automatizado de datos, lo que evidencia un desfase entre la normativa vigente y la realidad tecnológica actual.
4. Se concluyó que las entidades públicas presentan deficiencias en la implementación de la normativa de protección de datos personales, reflejadas en la ausencia de protocolos claros, limitada cultura institucional de protección de datos y problemas operativos en la gestión de información, lo que incrementa el riesgo de vulneración de derechos fundamentales.
5. Se determinó que existe una débil capacidad de control y supervisión por parte del Estado, así como una falta de claridad en la determinación de responsabilidades frente a vulneraciones, lo que debilita la eficacia del sistema de protección de datos personales en el sector público.

6. Se concluyó que la evolución de los sistemas de vigilancia digital en el sector público ha generado una tensión entre la seguridad pública y la protección de los derechos fundamentales, donde en la práctica suele prevalecer el interés estatal, evidenciando la necesidad de establecer un equilibrio basado en principios constitucionales.

RECOMENDACIONES

1. Se recomienda al Congreso de la República y a las entidades competentes incorporar una regulación específica sobre sistemas de vigilancia digital, incluyendo el uso de inteligencia artificial, reconocimiento facial y tratamiento automatizado de datos personales, a fin de reducir los vacíos legales existentes.
2. Implementación de evaluaciones de impacto (DPIA)
Se propone que las entidades públicas implementen evaluaciones de impacto en protección de datos personales antes de la adopción de sistemas de vigilancia digital, con el objetivo de prevenir riesgos y garantizar el respeto de los derechos fundamentales.
3. Fortalecimiento de la Autoridad Nacional de Protección de Datos Personales
Se recomienda fortalecer las competencias, recursos y capacidad sancionadora de la autoridad encargada, a fin de garantizar una supervisión efectiva del tratamiento de datos personales en el sector público.
4. Se sugiere que las entidades públicas elaboren e implementen protocolos claros y estandarizados para el tratamiento de datos personales en sistemas de vigilancia digital, asegurando el cumplimiento de los principios de legalidad, proporcionalidad y seguridad.
5. Se recomienda implementar programas de capacitación obligatoria para funcionarios públicos en materia de protección de datos personales y ética digital, con el fin de fortalecer la cultura institucional y prevenir vulneraciones.
6. Se propone establecer mecanismos de control más rigurosos, incluyendo auditorías periódicas, sistemas de trazabilidad de datos y mayores niveles de transparencia en el uso de tecnologías de vigilancia por parte del Estado.
7. Se recomienda establecer criterios normativos claros sobre la responsabilidad del Estado frente a vulneraciones de datos personales, a fin de garantizar mecanismos efectivos de reparación para los ciudadanos.

BIBLIOGRAFÍA

- Acevedo Paredes, M. Y., & Paredes Torres, K. A. (2024). *El efecto que causa la inteligencia artificial en la protección de datos personales bajo la Ley N.º 29733, Perú* (Tesis de pregrado). Universidad César Vallejo.
- Alexy, R. (2007). *Teoría de los derechos fundamentales*. Centro de Estudios Políticos y Constitucionales.
- Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.
- Bernal Pulido, C. (2007). *El principio de proporcionalidad y los derechos fundamentales*. Centro de Estudios Políticos y Constitucionales.
- Bernal Torres, C. A. (2016). *Metodología de la investigación* (4.^a ed.). Pearson Educación.
- Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.
- Carbonell, M. (2013). *Los derechos fundamentales en México*. Porrúa.
- Cassese, S. (2016). *La nueva Constitución económica*. Marcial Pons.
- Chorres Céspedes, C. A. (2024). *Impacto de la tecnología en la protección de datos personales desde el derecho constitucional* (Tesis de pregrado). Universidad Alas Peruanas.
- Congreso de la República del Perú. (1993). *Constitución Política del Perú*.
- Congreso de la República del Perú. (2011). *Ley N.º 29733, Ley de Protección de Datos Personales*.
- Córdova Abregú, A. F. (2023). *Tratamiento de datos personales en el marco de la atención de las solicitudes de acceso a la información pública* (Tesis de pregrado). Pontificia Universidad Católica del Perú.

Cotino Hueso, L. (2015). *Derecho público de las nuevas tecnologías*. Tirant lo Blanch.

Criado, J. I. (2016). Las administraciones públicas en la era digital. *Revista de Estudios Políticos*, 173, 11–38.

Criado, J. I., & Ramilo, M. C. (2003). E-administración: ¿Un reto o una nueva moda para las administraciones públicas? *Revista Vasca de Administración Pública*, 66, 11–44.

Davara Rodríguez, M. Á. (2014). *Derecho informático*. Aranzadi.

De Cupis, A. (1975). *Los derechos de la personalidad*. Bosch.

Eguiguren Praeli, F. J. (2019). *Derechos fundamentales y Constitución en el Perú*. Palestra Editores.

Ferrajoli, L. (2011). *Derechos y garantías: La ley del más débil*. Trotta.

Foucault, M. (2002). *Vigilar y castigar: Nacimiento de la prisión*. Siglo XXI Editores.

Frosini, V. (1984). *Informática y derecho*. Temis.

Gadamer, H.-G. (2012). *Verdad y método* (12.^a ed.). Ediciones Sígueme.

García Toma, V. (2013). *Derecho constitucional*. Adrus.

Gil-García, J. R., Helbig, N., & Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly*, 31, 11–18.

González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer.

Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. Oxford University Press.

Haro Benites, C. R., & Moncada Hernández, Y. C. (2024). *Constitucionalidad de la vigilancia masiva en el tratamiento de los datos personales en relación al derecho a la intimidad* (Tesis de pregrado). Universidad de Piura.

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2023). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (2.^a ed.). McGraw-Hill.

Landa Arroyo, C. (2017). *Derecho procesal constitucional*. Palestra Editores.

Larenz, K. (2010). *Metodología de la ciencia del derecho* (2.^a ed.). Ariel.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Martínez Martínez, R. (2007). *Protección de datos personales y derecho a la autodeterminación informativa*. Tirant lo Blanch.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mejía Arbildo, T. C. (2023). *Inteligencia artificial y sus efectos en la protección de datos personales en la Ley N.º 29733, Lima 2023* (Tesis de pregrado). Universidad César Vallejo.

Naciones Unidas. (2022). *E-government survey 2022: The future of digital government*. United Nations.

Pérez Luño, A. E. (2016). *Los derechos fundamentales en la sociedad tecnológica*. Tecnos.

Prieto Sanchís, L. (2003). *Justicia constitucional y derechos fundamentales*. Trotta.

Rebollo Delgado, L. (2010). *La protección de datos personales en el derecho europeo*. Dykinson.

Sagüés, N. P. (2011). *Derecho procesal constitucional*. Astrea.

Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

Tamayo y Tamayo, M. (2004). El proceso de la investigación científica (4.^a ed.). Limusa.

Troncoso Reigada, A. (2010). *La protección de datos personales: En busca del equilibrio*. Tirant lo Blanch.

Zagrebelsky, G. (2008). *El derecho dúctil*. Trotta.

Zedner, L. (2009). *Security*. Routledge.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

ANEXOS

LA PROTECCIÓN DEL DERECHO FUNDAMENTAL A LOS DATOS PERSONALES FRENTE AL USO DE SISTEMAS DE VIGILANCIA DIGITAL EN EL SECTOR PÚBLICO PERUANO			
Problema de investigación	Objetivos	Categorías / Subcategorías	Metodología
Problema general: ¿De qué manera se encuentra jurídicamente protegida la tutela del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano? Problemas específicos: a) ¿Cuáles son los límites jurídicos del tratamiento de datos personales por parte de las entidades del sector público mediante sistemas de vigilancia digital en el Perú?	Objetivo general: Analizar la protección jurídica del derecho fundamental a la protección de datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. Objetivos específicos: a) Determinar los límites jurídicos del tratamiento de datos personales por parte de las entidades del sector público mediante sistemas de vigilancia digital en el Perú. b) Identificar los vacíos o limitaciones del marco	Categoría 1: Protección del derecho fundamental a los datos personales - Protección constitucional de datos personales - Autodeterminación informativa - Principios del tratamiento de datos personales - Derechos del titular Categoría 2: Sistemas de vigilancia digital en el sector público - Concepto de vigilancia digital	Enfoque: Cualitativo. Tipo: Investigación básica. Nivel: Descriptivo–analítico. Diseño: No experimental, documental y transversal. Método: Jurídico-dogmático, hermenéutico y analítico. Técnicas: Análisis documental y entrevista. Instrumentos: Ficha de análisis documental y guía de entrevista. Población: profesionales especializados en derecho constitucional, derecho administrativo, derecho digital, protección de datos personales y gestión pública, tales como abogados, jueces, fiscales, funcionarios públicos, especialistas en

b) ¿Qué vacíos o limitaciones presenta el marco normativo peruano en la protección del derecho a los datos personales frente al uso de sistemas de vigilancia digital en la administración pública?	normativo peruano en la protección del derecho a los datos personales frente al uso de sistemas de vigilancia digital en la administración pública.	- Tipos de vigilancia digital - Vigilancia estatal y seguridad pública - Tratamiento de datos en la administración pública Categoría 3: Límites jurídicos del tratamiento de datos personales - Principio de legalidad - Principio de proporcionalidad - Límites del poder estatal - Control del tratamiento de datos Categoría 4: Vacíos del marco normativo	gobierno digital y académicos con conocimiento en la materia objeto de estudio Muestra: 10 expertos
--	--	---	--

		- Deficiencias regulatorias - Insuficiencia normativa frente a tecnologías digitales - Desafíos del gobierno digital	
--	--	--	--



FICHA DE ANÁLISIS DOCUMENTAL

FICHA DE ANÁLISIS DOCUMENTAL

1. Datos generales

- **Código de ficha:**
- **Tipo de documento:**
- **Título del documento:**
- **Autor / Institución:**
- **Año:**
- **Fuente:**

2. Categorías de análisis

- (✓) Protección de datos personales
- (✓) Garantías constitucionales
- (✓) Límites al poder del Estado
- (✓) Actuación del sector público
- (✓) Vacíos normativos

3. Contenido relevante

3.1. Resumen del contenido:

3.2. Extracto relevante (idea jurídica clave):



4. Análisis jurídico

4.1. Interpretación del contenido:

4.2. Relación con el problema de investigación:

4.3. Nivel de protección del derecho:

- ☐ Alto
- ☐ Moderado
- ☐ Limitado
- ☐ Insuficiente

Justificación:

5. Observaciones



GUÍA DE ENTREVISTA

I. Datos generales del entrevistado

- Código del entrevistado: _____
- Profesión: _____
- Especialidad: _____
- Institución donde labora: _____
- Cargo: _____
- Años de experiencia profesional: _____
- Fecha de entrevista: _____

II. Presentación

La presente entrevista tiene como finalidad obtener información especializada sobre la protección del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano. La información proporcionada será utilizada únicamente con fines académicos y se garantiza la confidencialidad de sus respuestas.

III. Preguntas de la entrevista

Categoría 1: Protección del derecho fundamental a los datos personales

1. Desde su perspectiva, ¿cómo se encuentra regulado el derecho fundamental a la protección de datos personales en el ordenamiento jurídico peruano?

2. ¿Considera que la normativa vigente garantiza adecuadamente la protección de los datos personales frente al uso de tecnologías digitales? ¿Por qué?

3. ¿Qué importancia tiene la autodeterminación informativa en la protección de los datos personales en el Perú?

Categoría 2: Sistemas de vigilancia digital en el sector público

4. ¿Cuál es su opinión sobre el uso de sistemas de vigilancia digital por parte de las entidades del sector público en el Perú?



UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

5.¿Qué riesgos identifica en el tratamiento de datos personales mediante sistemas de vigilancia digital por parte del Estado?

6.¿Considera que el uso de sistemas de vigilancia digital contribuye a la seguridad pública sin afectar derechos fundamentales? Explique.

Categoría 3: Límites jurídicos del tratamiento de datos personales

7.¿Cuáles considera que son los principales límites jurídicos que deben respetar las entidades públicas en el tratamiento de datos personales?

8.¿Considera que existen mecanismos efectivos de control del tratamiento de datos personales por parte del Estado? Fundamente.

Categoría 4: Vacíos del marco normativo

9.¿Qué vacíos o limitaciones identifica en la normativa peruana sobre protección de datos personales frente a sistemas de vigilancia digital?

10.¿Qué mejoras o reformas normativas propondría para fortalecer la protección del derecho a los datos personales en el sector público peruano?



ANEXO — CONSENTIMIENTO INFORMADO PARA PARTICIPACIÓN EN ENTREVISTA

CONSENTIMIENTO INFORMADO

Yo, _____, identificado(a) con DNI N.º _____, manifiesto que he sido informado(a) de manera clara, suficiente y comprensible sobre los objetivos y características de la investigación titulada:

“La protección del derecho fundamental a los datos personales frente al uso de sistemas de vigilancia digital en el sector público peruano”, realizada con fines exclusivamente académicos.

En ese sentido, declaro lo siguiente:

1. He sido informado(a) sobre el propósito de la investigación, el procedimiento de recolección de información y el uso que se dará a los datos proporcionados.
2. Entiendo que mi participación consiste en responder una entrevista sobre temas relacionados con la protección de datos personales y sistemas de vigilancia digital.
3. Mi participación es voluntaria y puedo retirarme en cualquier momento sin consecuencia alguna.
4. La información proporcionada será utilizada únicamente con fines académicos y de investigación.
5. Se garantiza la confidencialidad de mis respuestas y la protección de mi identidad, salvo autorización expresa para su divulgación.
6. No recibiré compensación económica por mi participación en el estudio.
7. Autorizo el uso de la información brindada para el análisis de resultados de la investigación.

En señal de conformidad, firmo el presente documento.

Datos del participante



UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

- Nombre completo: _____
- Firma: _____
- Fecha: ____ / ____ / ____

Datos del investigador

- Nombre del investigador: _____
- Firma: _____



UNIVERSIDAD NACIONAL DE SAN CR  BAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POL  TICAS

Creado el 14 de junio de 1979

ACTA DE SUSTENTACI  N DE TESIS DE LA ASPIRANTE FAYRUZ INGRID HINOSTROZA CUADROS

En la ciudad de Ayacucho, siendo las 11:00 a.m. del 29 de junio de 2026, reunidos en el auditorio de la Facultad de Derecho y Ciencias Pol  ticas-UNSCH, reunidos Richard Almonacid Zamudio (presidente), Iv  n Chumbe Carrera, Marlene Le  n Palacios, Jenny Juana Barraza Torres y Katherine Irma Quispe Vargas (miembros); reunidos para examinar la tesis. El derecho a la protecci  n de datos personales frente a sistemas de vigilancia digital en el sector p  blico peruano. Dando inicio a este acto acad  mico se designa como secretaria a la docente Katherine Irma Quispe Vargas acto seguido se procede a dar lectura a la Resoluci  n Decanal N   197-2026-UNSCH-FDCP-D y el art  culo 25 del reglamento de grados y t  tulos.

Acto seguido el presidente del jurado otorga el uso de la palabra a la aspirante, luego de la sustentaci  n se procede a realizar las preguntas y/o objeciones que el jurado considera pertinente; posteriormente se invita a la aspirante a salir del auditorio, acto seguido el jurado procede a deliberar.

El jurado decisi  n APROBAR POR UNANIMIDAD con la nota 11 (ONCE), concluye el acto acad  mico con la firma del acta; siendo las 13:00 a.m. de la ma  ana.

Richard Almonacid Zamudio

Iv  n Chumbe Carrera

Marlene Le  n Palacios

Katherine Irma Quispe Vargas

Jenny Juana Barraza Torres

**UNSCH****FACULTAD DE DERECHO
Y CIENCIAS POLITICAS****ESCUELA PROFESIONAL DE
DERECHO****CONSTANCIA DE ORIGINALIDAD N° 017-2026-UNSCH-FDCP**

El que suscribe responsable verificador de originalidad de trabajo de tesis de la Facultad de Derecho y Ciencias Políticas de la UNSCH, en cumplimiento a la Resolución de Consejo Universitario N.º 039-2021-UNSCH-CU (16-03-2021) Reglamento de Originalidad de Trabajos de Investigación de la UNSCH, otorga lo siguiente:

CONSTANCIA DE ORIGINALIDAD

Autor	Bach. FAYRUZ INGRID HINOSTROZA CUADROS
Para	Título profesional
Denominación de la tesis	El derecho a la protección de datos personales frente a sistemas de vigilancia digital en el sector público peruano.
Evaluación de Originalidad	25%
Numero de trabajo	2991776603
Fecha	30 de junio 2026

Amparo la presente en los artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación de la UNSCH, es procedente otorgar la constancia de originalidad con deposito.

Se expide la presente constancia a solicitud de la parte interesada para los fines que crea por conveniente.

Ayacucho, 30 de junio de 2026



Iván Chumbe Carrera

El derecho a la protección de datos personales frente a sistemas de vigilancia digital en el sector público peruano.

por Fayruz Ingrid HINOSTROZA CUADROS

El derecho a la protección de datos personales frente a sistemas de vigilancia digital en el sector público peruano.

INFORME DE ORIGINALIDAD

25%

INDICE DE SIMILITUD

26%

FUENTES DE INTERNET

20%

PUBLICACIONES

14%

TRABAJOS DEL ESTUD

FUENTES PRIMARIAS

1 hdl.handle.net

Fuente de Internet

2 www.informatica-juridica.com

Fuente de Internet

3 docta.ucm.es

Fuente de Internet

4 Submitted to D.A. de Derecho

Trabajo del estudiante

5 ruidera.uclm.es

Fuente de Internet

6 Submitted to Universidad Internacional de la Rioja

Trabajo del estudiante

7 www.tc.gob.pe

Fuente de Internet

8 ijj.ucr.ac.cr

Fuente de Internet

9 bdigital.uexternado.edu.co

Fuente de Internet

10 Submitted to Universidad Andina del Cusco

Trabajo del estudiante

11 cybertesis.unmsm.edu.pe

Fuente de Internet

12 idus.us.es

Fuente de Internet

13 Submitted to Integración Semipresencial

Trabajo del estudiante

14 Zamudio Salinas, Maria de Lourdes. "El Derecho a la Protección de Datos Personales de los Trabajadores Frente al Control Laboral a Traves del Sistema de Geolocalización GPS Límites y Propuestas", Pontificia Universidad Católica del Perú - CENTRUM Católica (Per

15 ifai.org.mx
Fuente de Internet

16 Submitted to Facultad Latinoamericana de Ciencias Sociales (FLACSO) - Sede Ecuador
Trabajo del estudiante

17 Flores Ostos, Saul Edgard. "La aplicación del control de convencionalidad difuso en la función fiscal y su repercusión en la administración de justicia en el Distrito Fiscal de Puno, 2024", Universidad Nacional del Altiplano de Puno (Peru), 2025
Publicación

18 Salas Palomino, Fiorella Stefany | Giles Magallanes, Rosa Cecilia. "Mejoras en la implementación del proceso de interoperabilidad en las entidades públicas", Pontificia Universidad Católica del Peru (Peru)
Publicación

19 Cossio Peralta, Andre Jorge. "El derecho a la intimidad en la vigilancia de la salud de los trabajadores", Pontificia Universidad Católica del Peru - CENTRUM Católica (Peru), 2021
Publicación

20 addi.ehu.eus
Fuente de Internet

21 Submitted to Universidad de Las Palmas de Gran Canaria
Trabajo del estudiante

22 Cuellar Villarroel, Luis Alberto. "El habeas data y la protección del derecho a la intimidad en los pronunciamientos del tribunal constitucional Peruano del año 1996 al 2011", Universidad Católica los Ángeles de Chimbote (Peru)
Publicación

23 Salome Resurreccion, Liliana Maria. "La "discriminacion multiple" como concepto juridico para el analisis de situaciones de discriminacion.", Pontificia Universidad Católica del Peru - CENTRUM Católica (Peru), 2021
Publicación