UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE CIENCIAS JURÍDICAS, CONTABLES Y SOCIALES

ESCUELA PROFESIONAL DE DERECHO

Tesis

El derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano, años 2020-2024

Asesor:

Dr. Chiclla Arredondo, Benedigto

Autor:

Reyes Zavala, Paulita Alexandra

Para optar el Título Profesional de Abogado

Abancay - Apurímac – Perú

2026

Universidad Tecnológica de los Andes

Transformando vidas

Acta N°: 001-2026

ACTA DE SUSTENTACIÓN DE TÍTULO PROFESIONAL

En la ciudad de Abancay, a los 04 días del mes de mayo del 2026, siendo las 10:00 horas, se reunieron los integrantes del Jurado designado por Resolución Directoral N° 0132-2026-UTEA-FCJCS-EPD de la Escuela Profesional de Derecho Facultad de Ciencias Jurídicas, Contables y Sociales:

Presidente :	Mag. Vasquez Elguera Roholly
Dictaminante:	Mag. Velazque Rojas Nilson Pastor
Replicante :	Mag. Ilaccaña Piérola Nestor

Para evaluar la sustentación, en la modalidad de:

☒ Tesis ☐ Trabajo de suficiencia profesional

Titulada:

El derecho fundamental de la autodeterminación informativa frente a la era digital en el sistema constitucional peruano años 2020-2024.

Desarrollado por el (los) Bachiller (es):

Br.: Reyes Zavala Paulita Alexandra
(Apellidos y Nombres)

Para optar el Título Profesional de:

Abogado
(Denominación del Título)

Concluido el acto, el Jurado dictaminó que el (la) (los) mencionado(a) (s) bachiller (es) fue (ron) APROBADO (S):

Por: Unanimidad
(Unanimidad o Mayoría) (*)

Emitiéndose el calificativo final de:

Bachiller (Apellidos y Nombres)	Calificación (**)
Br. Reyes Zavala Paulita Alexandra	Aprobada

Siendo las 12:40 horas concluyó la sesión, firmando los integrantes del Jurado.

Presidente: Mag. Vasquez Elguera Roholly
(Dr. Mg.). (Apellidos y Nombres)


(Firma)

Dictaminante: Mag. Velazque Rojas Nilson Pastor
(Dr. Mg.). (Apellidos y Nombres)


(Firma)

Replicante: Mag. Ilaccaña Piérola Nestor
(Dr. Mg.). (Apellidos y Nombres)


(Firma)

(*): Mayoría: Dos integrantes del jurado aprueban o desaprueban. Unanimidad: Todos los integrantes del jurado aprueban o desaprueban, Art.18 RGGAT.
(**): 0 a 10: Desaprobado, 11 a 13: Aprobado, 14 a 16: Aprobado con Buena, 17 a 20: Aprobado con Excelencia, Art. 18 RGGAT.

Reporte de similitud

21% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

15% Fuentes de Internet
12% Publicaciones
16% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos Complementarios

Datos del Autor		
Apellidos y Nombres	:	Reyes Zavala, Paulita Alexandra
Tipo de Documento de Identidad	:	DNI
Número de Documento de Identidad	:	76512990
URL ORCID	:	https://orcid.org/0009-0003-1595-8510
Datos del Asesor		
Apellidos y Nombres	:	Chiclla Arredondo, Benedigto
Tipo de Documento de Identidad	:	DNI
Número de Documento de Identidad	:	31019408
URL ORCID	:	https://orcid.org/0000-0001-8519-6791
Datos de la Investigación		
Facultad	:	Ciencias Jurídicas, Contables y Sociales
Escuela profesional	:	Derecho
Línea de investigación	:	Derecho Privado y Público
Rango de años en que se realizó la investigación	:	2023-2025
Fuente de financiamiento	:	Autofinanciado
Porcentaje de similitud	:	21% con depósito
URL de OCDE	:	https://purl.org/pe-repo/ocde/ford#5.05.01

Dedicatoria

Por darme la fortaleza, y coraje a Dios, asi también a mi querido padre Gerry Meléndez Trujillo, quién tenía la fe, constancia y dedicación en fortalecer el sistema constitucional peruano.

Agradecimiento

Expreso mi gratitud a mi asesor de investigación, por toda su orientación, y dedicación constante en mi investigación. Muchas gracias por toda su paciencia.

Resumen

La autodeterminación informativa, como derecho constitucional faculta a toda persona a gestionar sus datos personales en bases públicas o privadas, abarcando aspectos como el acceso, consulta del uso, identificación de recopiladores, actualización y supresión cuando se vulneran otros derechos. No obstante, el vertiginoso avance digital ha dejado rezagada la normativa actual, evidenciando fallos en entidades públicas y privadas que no garantizan confidencialidad, ni mecanismos idóneos, exponiendo a la ciudadanía al procesamiento masivo de datos.

Esta investigación analiza si el ordenamiento constitucional peruano resguarda adecuadamente este derecho ante los retos digitales. Se concluye que sí lo protege, aunque con limitaciones prácticas que exigen reformas urgentes. Entre ellas, destacan la escasa preparación de jueces en materias tecnológicas y la ineficacia del proceso de hábeas data, prolongada e ineficaz para disputas digitales. Se examina la regulación dispersa desde la Constitución hasta las leyes inferiores, y la adaptación progresiva del marco digital, impulsada por políticas gubernamentales de los últimos siete años que integran la tecnología en la gestión pública.

Como vías de fortalecimiento, se propone optimizar el hábeas data para contrarrestar las tecnologías emergentes tales como el análisis de datos masivo, y la inteligencia artificial; armonizar el marco legal bajo una perspectiva integral; y promover la articulación entre el Poder Judicial y el ente rector de la protección de datos personales, dando prioridad a la capacitación y tutela jurisdiccional efectiva. Empleando un enfoque cualitativo, se revisaron fallos del Tribunal Constitucional y normas vigentes, con miras a potenciar esta garantía en el contexto digital actual.

Palabras Claves: Autodeterminación, Era digital, Sistema Constitucional Peruano.

Abstract

Informational self-determination, as a constitutional right, empowers every person to manage their personal data held in public or private databases, encompassing aspects such as access, consultation regarding its use, identification of data collectors, updating, and deletion when other rights are violated. However, the rapid pace of digital advancement has left current regulations lagging, revealing shortcomings in public and private entities that fail to guarantee confidentiality or adequate mechanisms, exposing the population to cyber risks and massive data trafficking.

This research analyzes whether the Peruvian constitutional order adequately safeguards this right in the face of digital challenges. It concludes that it does protect it, albeit with practical limitations that demand urgent reforms. Among these limitations are the lack of training of judges in technological matters and the ineffectiveness of the habeas data process, which is lengthy and ineffective for digital disputes. The study examines the scattered regulations, from the Constitution to lower-level laws, and the progressive adaptation of the digital framework, driven by government policies of the last seven years that integrate technology into public administration.

As ways to strengthen this right, it is proposed to optimize habeas data to counteract emerging technologies such as big data analytics and artificial intelligence; harmonize the legal framework from a comprehensive perspective; and promote collaboration between the Judiciary and the governing body for personal data protection, prioritizing training and effective judicial protection. Using a qualitative approach, rulings of the Constitutional Court and current regulations were reviewed, with a view to strengthening this guarantee in the current digital context.

Keywords: Self-determination, Digital age, Peruvian constitutional framework.

Índice general

Portada……i

Acta de sustentación ii

Reporte de similitud iii

Metadatos Complementarios iv

Dedicatoria..... v

Agradecimiento vi

Resumen vii

Abstract..... viii

Índice general ix

Índice de tablas xii

Índice de anexos xiii

I. Introducción 15

II. Planteamiento del problema 17

2.1 Descripción y formulación del problema 17

2.1.1 Descripción del problema..... 17

2.1.2 Formulación del problema de investigación 25

2.1.2.1 Problema general:..... 25

2.1.2.2 Problemas específicos: 25

2.2. Objetivos 25

2.2.1. Objetivo general 25

2.2.2. Objetivos específicos..... 25

2.3. Justificación e importancia..... 26

2.4. Categorías de análisis. 27

III. Marco teórico 29

3.1 Antecedentes 29
3.1.1. Antecedentes internacionales 29
3.1.2. Antecedentes nacionales 31
3.1.3. Antecedentes regionales y locales 33
3.2 Bases teóricas 33
3.3 Definición de términos 50
IV. Metodología 54
4.1. Tipo y nivel de investigación 54
4.1.1 Tipo de investigación 54
4.1.2 Nivel de investigación 54
4.2 Ámbito temporal y espacial 55
4.3 La población y muestra 55
4.4 Instrumentos 56
4.4.1. Técnica de recolección de la información 56
4.4.2. Instrumento de recolección de información 57
4.5 Procedimientos 58
4.6 Análisis de datos 58
4.7 Consideraciones éticas 59
V. Resultados y discusión 60
5.1. Resultados de la entrevista 60
5.2. Resultado del análisis jurisprudencial. 68
5.3. Resultado de análisis normativo. 72
5.4. Discusión de resultados 75
5.5. Triangulación de datos. - Derecho a la autodeterminación informativa y la era digital en el sistema constitucional peruano. 100

VI. Conclusiones..... 108

VII. Recomendaciones..... 111

VIII. Referencias 113

IX. Anexos..... 119

Índice de tablas

Tabla 1: Categorías y sub categorías del estudio..... 27

Tabla 2: Cuadro de transcripción de respuestas de entrevistados (Jueces) 60

Tabla 3: Cuadro de transcripción de respuestas de entrevistados (Ingenieros)..... 65

Tabla 4:Cuadro de análisis de sentencias de habeas data emitidas por el Tribunal Constitucional relacionadas con la era digital. 71

Tabla 5: Cuadro de fuentes y enfoques 100

Tabla 6: Esquema de resumen de triangulación 101

Índice de anexos

Anexos 1 Matriz de consistencia categorial 119

Anexos 2 Ficha de validación de instrumentos de recolección de datos juicio de expertos 120

Anexos 3 Consentimiento y asentimiento informado de la entrevista 121

Anexos 4 Preguntas para los jueces civiles o constitucionales 122

Anexos 5 Preguntas para los ingenieros del área de soporte informática del poder de judicial de Apurímac y/o Cusco 126

Anexos 6 Evidencias de ejecución y recolección de datos..... 129

Anexos 7 Resolución Final N°034-2020/CC3 (INDECOPI) 160

Anexos 8 Caso: Aguedo Zuñiga Sebastián Carlos Vs Ministerio del Interior 188

Anexos 9: Muñoz Salazar Edwar Antonio Vs Usuario de Facebook..... 211

Anexos 10 Caso: Juan Mejia Seminario VS Mark Zuckerberg 233

Anexos 11 Caso: Reservado..... 243

Anexos 12 Caso: Apaza Suca Francisco Romulo VS Movistar..... 256

Anexos 13 Caso: Derrama Magisterial Apurímac..... 289

Anexos 14 Ley de Protección de datos personales Ley N°29733 y su Reglamento (Derogado)..... 326

Anexos 15 D.S N°016-2024-JUS Reglamento de la Ley N°29733 357

Anexos 16 Decreto Legislativo N°1412..... 382

Anexos 17 Decreto de Urgencia N°006-2020 388

Anexos 18 Decreto de Urgencia N°007-2020 392

Anexos 19 Reglamento del Decreto Legislativo N°1412..... 397

Anexos 20 Decreto que aprueba la Política Nacional de Transformación Digital al 2030 434

Anexos 21 Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. 462

I. Introducción

La autodeterminación informativa, como derecho fundamental reconocido en el sistema constitucional se configura como base crucial para proteger la intimidad, la privacidad y la dignidad humana en el contexto digital. Este privilegio, reconocido en múltiples sistemas legales, confiere a los individuos la potestad de administrar el manejo, acceso y divulgación de su información personal. Dentro del sistema constitucional peruano, la autodeterminación informativa ha adquirido una importancia mayor, especialmente durante el período 2020-2024, donde la transformación digital ha reconfigurado el alcance del derecho a la autodeterminación informativa, al introducir problemas que el ordenamiento peruano aún busca resolver.

La era digital ha tejido un universo donde la recolección, almacenamiento y manipulación de información personal se llevan a cabo a una magnitud inédita. El vasto océano de datos que manejan corporaciones, gobiernos y plataformas digitales puede desencadenar riesgos serios para el ejercicio efectivo de este derecho dentro de un entorno digital.

La finalidad del derecho fundamental a la autodeterminación informativa no es solo que los individuos puedan elegir cómo se utilizan sus datos, sino también evitar actos inapropiados como el hurto de identidad, la discriminación algorítmica, filtración de datos y la manipulación de la percepción pública.

En el sistema constitucional peruano, y salvaguarda de este derecho ha ganado relevancia en tiempos recientes, impulsada por la instauración de regulaciones y veredictos judiciales que buscan conciliar la era digital y la protección de los derechos fundamentales.

La normativa peruana relacionada con la salvaguarda de los datos de carácter personal y las políticas de ciberseguridad ha sido un terreno de constante evolución y

transformación, con la finalidad de fortalecer la autonomía de los individuos bajo las nuevas dinámicas impuestas por la era digital.

Esta investigación analiza la autodeterminación informativa en el Perú como garantía constitucional frente al tratamiento de datos en entornos digitales, examinando su metamorfosis legal, los principales obstáculos que enfrenta y su repercusión en la comunidad. La importancia de mi estudio se centra en analizar de qué manera la protección constitucional puede adaptarse a los cambios tecnológicos, buscando que la autodeterminación informativa permanezca como garantía irrenunciable del individuo en la sociedad digital.

La investigación se descompone en nueve capítulos, que a continuación detallo:

En el primer capítulo se abordó la presentación. En el segundo capítulo, se abordó la formulación del problema, la descripción de la realidad en cuestión, los objetivos, la razón y relevancia de la investigación, las categorías. En el tercer capítulo se abordó todo lo relacionado con la base teórica, los cimientos teóricos y la definición de conceptos. En el cuarto capitulo se abordó la metodología, el tipo y nivel de estudio, el espacio temporal y espacial del estudio, la población y la muestra, los instrumentos, el procedimiento, la interpretación de datos y las reflexiones éticas. En el quinto capítulo, nos sumergimos en los resultados y la discusión. La conclusión emergió en el sexto capitulo. En el séptimo capítulo, la sugerencia. En el octavo capitulo se incluyen las referencias y, finalmente, en el noveno se incluyen los anexos.

II. Planteamiento del problema

2.1 Descripción y formulación del problema

2.1.1 Descripción del problema

Actualmente nuestra sociedad experimenta un período de cambios acelerados, y la opción para lograr su supervivencia es la adaptación como parte de la naturaleza humana y su evolución biológica. Uno de esos cambios ha sido impulsado por la ciencia y la tecnología; es lo que podría llamarse la revolución digital, la cual ha traído novedades sin límites, ya sea para facilitar nuestra vida social, laboral, personal y otros.

Desde los grandes inventos del hombre como la computadora de Konrad Zuse en 1941, el sistema operativo Windows de Bill Gates, el teléfono móvil de Steve Jobs, los buscadores de Google creación de Larry Page y Sergey Brin, la creación de las redes sociales como Facebook de Mark Zuckerberg, el Chat GPT de Elon Musk que viene a ser la invención de invenciones de esta década, y otras creaciones de innumerables prestigiosos investigadores, nos demuestran que nuestro único límite viene a ser nuestra imaginación.

Así, los grandes inventos tecnológicos han ido dando paso al surgimiento de la era digital que ha ido ocupando y convirtiéndose en una necesidad del día a día del ser humano, donde la pandemia acelero todo; y a partir del año 2020 el Estado opto por la prestación de servicios al ciudadano en forma digital.

A fin de acceder al mundo digital las personas requieren de ciertos componentes como la conexión a internet ya sea a través del WI-FI o datos móviles, así también se requiere de aparatos electrónicos como los teléfonos móviles, computadoras y otros, cabe destacar que a partir del uso de aparatos electrónicos y su conexión a internet se da paso al gran flujo de datos que son analizados por el Big Data a través de algoritmos electrónicos que son

alimentados por todas las personas a través del acceso a sus redes sociales, sus búsquedas en internet y otros; bajo una falacia de gratuidad.

Si bien la Inteligencia Artificial optimiza procesos sociales y económicos, su implementación sin salvaguardas expone a los ciudadanos a formas emergentes de afectación de derechos, tales como el uso no autorizado de su imagen, voz o identidad digital.

Estos avances, sin embargo, no son fácilmente adaptables a las reglas para que la sociedad conviva pacíficamente, dentro del marco de un Estado de Derecho donde los derechos de la persona son el núcleo central del Estado. Hasta este punto, es posible que nos preguntemos ¿Y cómo se está desarrollando y evolucionando de una forma tan acelerada el mundo digital?

Si bien la respuesta es simple a partir de un "dato", en el mundo digital cada dato aportado contiene información relacionada a nuestra vida privada, un ejemplo de ello es el uso de las redes sociales donde se comparten imágenes, reacciones a publicaciones, mensajes privados y públicos (comentarios), notas de voz, transmisiones en vivo y otros; así también, nuestras búsquedas en Google u otros buscadores, permiten a través de los algoritmos saber nuestros intereses, ubicación, lo que hacemos e incluso hasta como nos sentimos; y todo dato aportado es almacenado por los propietarios de las páginas web, redes sociales y otros, a fin de ser comercializados, a cambio de la prestación del uso de la Web, redes sociales y otras herramientas virtuales necesarias del ser humano.

Establecer un momento en el que los algoritmos empiezan a procesar los datos sería a partir desde la adquisición de productos tecnológicos como los teléfonos móviles, computadoras y otros, productos que requieren de sistemas operativos(como Android, IOS y otros para celulares; y Windows, Mac OS, y otros para computadoras) para un debido funcionamiento; cabe aclarar que estos sistemas tienen acceso a nuestras agendas

telefónicas, galería de imágenes, audio, cámara, mensajes y otras funciones que te ofrecen estas tecnologías; sucesivamente sería con la descarga de aplicaciones como las redes sociales, y aplicaciones, donde el acceso y uso de estas requieren la aceptación de las condiciones de privacidad, siendo esta última una especie de un contrato de adhesión suscrita bajo la normativa del país de origen de la aplicación, caso contrario no se puede hacer uso de ellas; y por último se requiere el servicio de internet.

En el Perú vemos que muchos empresas y entidades no cuidan cautelosamente los datos, afectando información que hace identificable a un individuo: datos de identidad, edad, medios de contacto y características biométricas; lo que está dando lugar que muchos ciudadanos peruanos se vean afectados con este mal uso, ya sea desde recibir llamadas telefónicas ofreciendo servicios de cualquier naturaleza conocida como “Spam”, e incluso recibiendo mensajes ya sean telefónicos o por correo electrónico, donde instituciones como INDECOPI tuvieron que tomar manos en el asunto y multar a las empresas que realizaron llamadas sin consentimiento de sus titulares; entre ellos tenemos el caso del Banco Pichincha donde la Comisión de Protección al Consumidor N°3 mediante Resolución N°034-2020/CC3, impuso una sanción de 45 UIT (Unidad Impositiva Tributaria), por realizar comunicaciones sin el consentimiento de los usuarios.

El meollo del asunto radica en preguntarnos ¿Cómo estas empresas tuvieron acceso a estos datos?, la respuesta es la inseguridad virtual, y el tráfico masivo de datos, pero la importancia radica en que estos datos merecen protección legal adecuada dada a su naturaleza, con lo cual debe garantizarse que estos datos no caigan, ni sean ventiladas a personas inescrupulosas que pueden dar mal uso de estas, incrementando la exposición del ciudadano a modalidades delictivas propias del entorno digital, como el robo de datos, la falsedad de identidad y el engaño informático.

Así mismo, diariamente los peruanos somos consumidores de información de toda clase de naturaleza en el mundo virtual, información que no está sujeta a filtros de veracidad, con lo cual los usuarios pueden dar por ciertas ese tipo de información e influir en sus decisiones del día a día. Hasta este punto los navegantes de internet somos proveedores de datos y a la vez consumidores de información.

El torrente de información en el universo digital no conoce límites, y el gran mercado que mueve la economía a nivel mundial del ahora y el mañana son los datos; los datos son sinónimo de poder, dado que estos últimos están intrínsecamente ligados a la intimidad y la esencia de la existencia humana, con lo cual se puede predecir comportamientos, gustos, e incluso decisiones políticas a través del procesamiento de datos a nivel masivo, ejemplo de ello es el polémico caso ocurrido en el año 2016 conforme a la revista "The Guardian" donde se revelo que se utilizó 50 millones de perfiles de usuarios de Facebook a fin de influir en las elecciones presidenciales, a través de anuncios personalizados que los influyan a votar por el candidato Donal Trump. (Guardian, 2018).

El contexto desarrollado obliga a reafirmar el contenido esencial de la autodeterminación informativa como límite al tratamiento de datos, en particular cuando su uso puede incidir en la formación de la voluntad electoral.

El Derecho, en su función de regular las relaciones entre personas, debe afrontar los avances científicos y tecnológicos, adaptándose a ellos y garantizando que se desarrollen respetando los derechos fundamentales.

En este momento es crucial plantear cuál es el papel del Estado en la salvaguarda de los datos en la era digital, más aún cuando estos datos se encuentran bajo la administración de empresas internacionales y nacionales, públicas y privadas, así también se debe conocer cuáles son los mecanismos con los que cuentan las personas para poder autotutelar su

información personal y, además, qué hacer cuando información valiosa se filtra al público o es usada indiscriminadamente en el mercado.

En ese sentido, lo que se espera del Estado es que no solamente regule conductas de los ciudadanos a través de normas sustantivas, sino que también se dicten normas adjetivas que optimicen la vivencia de los derechos fundamentales; aquí el Estado debe cumplir un fin tutelando, previniendo y sancionando conductas dañosas.

Sobre protección de datos personales, aun faltan investigaciones exhaustivas que vinculen la necesidad de un marco constitucional para su protección frente a la era digital, que avanza a grandes pasos y muy rápidamente. Justamente mi objetivo de investigación se enfoca en analizar el estado de cosas actual, de modo que se pueda iniciar algunos proyectos conducentes a mejorar el sistema normativo vigente en el contexto del avance de la era digital.

La autodeterminación informativa goza de reconocimiento constitucional en el Perú, conforme al artículo 200 inciso 3 de la Constitución que consagra el hábeas data como garantía procesal, en armonía con tratados internacionales suscritos por el Estado. Su desarrollo legal se encuentra en la Ley N.º 29733, Ley de Protección de Datos Personales, reglamentada por el Decreto Supremo N.º 016-2024-JUS, mientras que la tutela jurisdiccional específica se regula en el Título IV del Nuevo Código Procesal Constitucional.

Del bloque normativo que regula la autodeterminación informativa en el Perú, se advierte una asimetría temporal: mientras la Constitución data del 1993, la Ley N.º 29733 del 2011 y el Nuevo Código Procesal Constitucional del 2021, el único instrumento reciente es el Decreto Supremo N.º 016-2024-JUS que reglamenta la Ley de Protección de Datos Personales. Este reglamento, según su exposición de motivos, busca reforzar la tutela preventiva frente a riesgos derivados de las tecnologías emergentes. No obstante, la

existencia de un marco normativo mayoritariamente anterior a la masificación de la inteligencia artificial, big data y plataformas digitales evidencia un desfase regulatorio. La problemática radica en que la protección efectiva de la autodeterminación informativa exige no solo normas vigentes, sino instrumentos con capacidad técnica para responder a vulneraciones propias de la sociedad digital, lo cual compromete tanto el ejercicio ciudadano de este derecho como la función garantista del Estado.

El ejercicio efectivo de la autodeterminación informativa en el Perú se ve limitado por prácticas institucionales que contravienen el principio de seguridad. Organismos públicos y empresas privadas mantienen niveles insuficientes de cumplimiento normativo, lo que deriva en incidentes de seguridad que comprometen datos de carácter personal.

En la actualidad tenemos casos recientes que ha evidenciado la filtración de datos de forma masiva como es el caso del Banco Interbank que en octubre del año 2024, su sistema de seguridad fue objeto de filtración por parte de un tercero que obtuvo acceso a datos de tres millones de clientes, este hecho evidencio la vulnerabilidad del sistema de seguridad de datos de las entidades privadas frente a este tipo de ataques cibernéticos, así también, reflejo la importancia de proteger los datos en un entorno digital y robustecer las medidas de protección ante este tipo de amenazas. (Nolasco, 2024).

Sobre esto, el Tribunal Constitucional estableció como criterio de interpretación que la autodeterminación informativa se ve lesionada cuando responsables del tratamiento, sean del sector público o privado, realizan tratamiento no consentido, transferencias indebidas o exponen datos personales sin habilitación legal (STC Exp. N.º 02839-2021-PHD/TC, 2021).

En dicha sentencia, el Colegiado determinó la responsabilidad de la Dirección de Criminalística de la PNP por incumplir sus deberes de custodia, al permitir que la empresa VOCATI CONSULTING accediera de forma irregular a sus registros institucionales. Dicha

exposición de información del demandante generó una afectación concreta a su esfera laboral y configuró una vulneración al derecho previsto en el artículo 2 inciso 6 de la Constitución.

Se advierte que la exposición de datos personales obedece al incumplimiento de medidas de seguridad por responsables públicos y privados, quienes ejecutan tratamientos sin consentimiento del titular. Esta omisión genera una amenaza permanente a la autodeterminación informativa y demás derechos conexos.

Asimismo, si bien el ordenamiento constitucional peruano prevé el hábeas data como mecanismo procesal específico para tutelar la autodeterminación informativa frente al tratamiento no consentido de información en bancos de datos, este instrumento exhibe limitaciones para brindar protección eficaz. El proceso constitucional encuentra obstáculos ante fenómenos propios de la sociedad digital, tales como el procesamiento automatizado a gran escala y las intrusiones informáticas, los cuales pueden lesionar el derecho tanto en su dimensión individual como colectiva.

En el ámbito constitucional, el ejercicio del hábeas data se encuentra condicionado al cumplimiento del requisito previo de solicitud directa ante el responsable del tratamiento, requiriéndose la petición de acceso, rectificación, supresión u oposición y la obtención de una respuesta denegatoria o relativamente parcial transcurrido el plazo de diez días hábiles previsto en el artículo 69 inciso 3 del Decreto Supremo N.º 016-2024-JUS. Dicha exigencia dilata la tutela jurisdiccional efectiva, situación que se agrava cuando entidades públicas o privadas invocan indebidamente cláusulas de reserva o confidencialidad para denegar información, tal como ocurrió en la STC Exp. N.º 01116-2022-PHD/TC, donde Telefónica del Perú S.A.A. se rehusó brindar datos sobre la titularidad de líneas telefónicas vinculadas a llamadas reiteradas dirigidas al demandante.

Dentro del sistema constitucional, el proceso de tutela de datos es el procedimiento principal y de mayor jerarquía para garantizar el respeto al derecho a la autodeterminación informativa. No obstante, su ejercicio enfrenta barreras formales como el requisito de reclamo previo, que obliga al titular haber solicitado previamente la defensa de su derecho mediante un documento con fecha cierta, y que la entidad rechace esa solicitud. Además, existen plazos estrictos, como el límite de 60 días desde la negativa para presentar la acción judicial, lo que implica que, si el titular no actúa dentro de ese plazo, pierde la posibilidad de reclamar su derecho.

En esa misma línea, también existe la barrera formal del emplazamiento en el proceso de tutela de datos cuando se trata de ejercer la defensa del derecho a la autodeterminación informativa frente a empresas internacionales, ya que por este proceso, el emplazamiento se dificulta dada la jurisdicción limitada, y la falta de mecanismos efectivos que permitan notificar a estas empresas, garantizando el debido proceso; y en el mismo sentido la dificultad de hacer efectivo que las empresas internacionales cumplan con lo resuelto en la sentencia.

En dicho escenario, pese a que el hábeas data fue creado normativamente como un proceso de tutela urgente, preferente y sumario, en la práctica jurisdiccional su tramitación excede los plazos legales. Esta demora resulta incompatible con la naturaleza del derecho a la autodeterminación informativa, que exige tutela judicial inmediata ante vulneraciones derivadas del tratamiento automatizado de información personal, especialmente en un contexto de transformación tecnológica acelerada.

En este sentido, es necesario que el Estado peruano, a través de sus diferentes poderes, promulgue normativas adecuadas que no obstaculicen el progreso tecnológico, sino

que además aseguren una tutela eficaz frente a posibles situaciones que puedan afectar su derecho a la autodeterminación informativa de los ciudadanos.

2.1.2 Formulación del problema de investigación

2.1.2.1 Problema general:

- ¿De qué manera es protegido el derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano?

2.1.2.2 Problemas específicos:

- ¿De qué manera se protegen los datos personales generales frente a la era digital en el sistema constitucional peruano?
- ¿De qué manera se encuentran protegidos los datos sensibles frente a la era digital en el sistema constitucional peruano?
- ¿Cómo se regula el consentimiento informado frente a la era digital en el sistema constitucional peruano?

2.2. Objetivos

2.2.1. Objetivo general

- Analizar la protección legal del derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano.

2.2.2. Objetivos específicos

- Describir de qué manera se protegen los datos personales generales frente a la era digital en el sistema constitucional peruano.
- Explicar de qué manera se encuentran protegidos los datos sensibles frente a la era digital en el sistema constitucional peruano.
- Determinar cómo se regula el consentimiento informado frente a la era digital en el sistema constitucional peruano.

2.3. Justificación e importancia

2.3.1. Justificación de la investigación

2.3.1.1. Justificación teórica.

La justificación teórica se sustenta en la relevancia de examinar los mecanismos constitucionales de tutela de la autodeterminación informativa frente a los riesgos emergentes del entorno digital. Este derecho faculta al titular a ejercer control sobre el flujo de su información personal, impidiendo que responsables del tratamiento, con independencia de su naturaleza jurídica o ubicación territorial, destinen los datos a finalidades incompatibles con las autorizadas.

Según Hernández Sampieri (2014), la justificación teórica permite sustentar conceptualmente el problema de investigación, identificando los marcos legales, doctrinarios y contextuales que lo explican. Así, este trabajo parte del análisis de teorías jurídicas y constitucionales relacionadas con la protección de datos, articuladas con el enfoque cualitativo para interpretar discursos normativos, institucionales y sociales. En consecuencia, se busca aportar una comprensión crítica sobre cómo se manifiesta y garantiza este derecho en el Perú, frente a la expansión digital y el tratamiento masivo de información personal.

2.3.1.2. Justificación práctica

La presente investigación tiene como justificación practica la necesidad de conocer, comprender y abordar las problemáticas que trae la era digital, especialmente ante casos de uso indebido de datos, filtración, y exposición de datos sin el consentimiento de sus titulares en un contexto digital.

La justificación practica desde la perspectiva del sujeto de derecho, permitirá abordar los mecanismos legales con los que cuentan dentro del sistema constitucional, a fin de proteger sus datos personales ante casos como filtraciones, hackeos, y exposición de sus

datos, frente a la vulnerabilidad de los usuarios y la insuficiente protección efectiva de los derechos en un entorno digital.

2.3.1.3. Justificación metodológica

La opción por el enfoque cualitativo se justifica en su aptitud para examinar la configuración normativa y eficacia práctica de la autodeterminación informativa, particularmente en escenarios de procesamiento masivo de información personal dentro del marco constitucional vigente.

Este enfoque permite explorar significados, percepciones y prácticas jurídicas en su contexto social y normativo. Según Hernández Sampieri (2014), la justificación metodológica explica por qué se selecciona un determinado enfoque para abordar el problema de investigación de manera coherente con sus características. En este caso, se utilizarán técnicas como el análisis documental y entrevistas a expertos, para captar la complejidad del fenómeno desde una perspectiva interpretativa.

2.3.1.4. Justificación legal

La justificación legal de mi estudio radica en la necesidad de mejorar la protección legal del derecho a la autodeterminación informativa, considerando los desafíos que presenta la era digital. Esto exige un análisis minucioso para asegurar que el marco legal actual sea efectivo frente a futuras vulneraciones a este derecho.

Jurídicamente, este trabajo va a generar criterios interpretativos para la doctrina y el legislador, evidenciando la urgencia de actualizar los mecanismos de protección de la autodeterminación informativa ante la transformación ante un entorno digital, garantizando que el uso de datos personales se subordine al respeto de los derechos.

2.4. Categorías de análisis.

Conforme al diseño metodológico adoptado, se definen las siguientes categorías:

Tabla 1: *Categorías y subcategorías de estudio conforme a mi matriz categorial.*

Categorías de análisis.	**Definición conceptual**	**Subcategorías**
Categoría 1: Derecho fundamental a la autodeterminación informativa.	Por este derecho se reconoce la capacidad de determinar el destino de los datos personales, desde su captación hasta su eliminación, en cualquier soporte o sistema de tratamiento.	-Datos personales generales. -Datos personales sensibles. -Consentimiento informado.
Categoría 2: Era digital en el sistema constitucional peruano.	Contexto social que se caracteriza por el uso de tecnologías digitales, que permiten recopilar, procesar y circular datos personales; y su regulación dentro del sistema constitucional peruano.	-Políticas de Gobierno Digital. -Riesgos digitales. -Mecanismos de Tutela jurisdiccional.

III. Marco teórico

3.1 Antecedentes

3.1.1. Antecedentes internacionales

Viveros (2018),en su tesis, bajo el título “Derecho a la autodeterminación informativa sobre los datos genéticos”, para optar el grado de Magister en Derecho y Nuevas Tecnologías en la Universidad de Chile, se propuso explorar si la normativa chilena cuida adecuadamente la salvaguarda de los datos personales que constituyen la intimidad biológica. Para llevar a cabo su investigación, optó por una metodología esencial, con un enfoque descriptivo. Su estudio reveló que la metamorfosis de las tecnologías de la información y la comunicación ha provocado que el manejo de datos personales pueda impactar la intimidad personal; aunque la legislación chilena protege la intimidad personal, el derecho a la privacidad genética no tiene regulación específica, por lo tanto, es posible que sea vulnerado en el tratamiento indiscriminados de estos.

Pérez et al. (2019), en su tesis “La regulación del derecho a la autodeterminación informativa en El Salvador”, para optar el grado de licenciado en Ciencias Jurídicas de la Universidad de El Salvador, se propuso desentrañar la evolución de la recopilación de información personal a lo largo de la historia y desentrañar cómo la tecnología transformó la habilidad para guardar, procesar y tratar los datos recopilados. A través de una indagación fundamental, con un enfoque descriptivo, concluyeron que, en el Salvador, el derecho a la autodeterminación informativa ha florecido mediante diversas leyes, aunque su carácter singular limita su aplicación, dejando fuera una porción de la realidad social que demanda una normativa que aborde el tratamiento de datos personales. Por ello, es imperativo instaurar una normativa que aborde de manera directa la protección de datos personales. (pág. 123)

Canizales (2021), en su tesis titulada “La eficacia Horizontal de los derechos humanos, el caso del derecho a la autodeterminación informativa” para optar el grado de Magister en derecho procesal constitucional en la Universidad Panamericana de México. En su estudio sobre el derecho a la autodeterminación informativa buscó reafirmar la influencia de los derechos humanos en las interacciones humanas, examinando la normativa vigente para sugerir el amparo como herramienta constitucional para vigilar las transgresiones de la privacidad personal. Realizó una indagación fundamental, empleando un enfoque descriptivo y una metodología cualitativa. Al concluir su investigación, concluyó que el progreso tecnológico, la sencillez en la obtención de información, han facilitado la recolección de datos, la inmediatez de la transferencia de estos, la posibilidad de un mal uso coloca a sus titulares en una posición vulnerable frente a la violación de su derecho a la autodeterminación informativa.

Manzano (2021), en su tesis titulada “El habeas data y los derechos de protección de datos personales en Ecuador" para optar el grado de magister en la Universidad Nacional de Tumbes, buscó desentrañar cómo los juristas ven las protecciones legales del habeas data y cómo se ven afectados los derechos de los datos personales. La investigación llevada a cabo fue de carácter básico, con un enfoque descriptivo, y concluyó que el ciudadano percibe y siente que su derecho a la protección de su información personal está en riesgo, lo cual revela que no ha ejercido plenamente su derecho a la autodeterminación informativa y la efectiva acción del habeas data.

Chura (2022), en su disertación denominada "La necesidad de incorporar la autodeterminación informativa como derecho esencial en la Constitución Política del Estado", para obtener el grado académico de Abogada en la Universidad Mayor de San Andrés en Bolivia, se propuso llevar a cabo una reforma constitucional que reconociera la autodeterminación informativa como derecho esencial, brindando a la información una

protección digna, los datos personales y el procesamiento digital de la información. Realizó una investigación básica, con un enfoque descriptivo. Sus principales conclusiones fueron las siguientes:

1) Al carecer de una defensa adecuada, el derecho a la autodeterminación informativa podría verse comprometido por los avances tecnológicos, impactando así los derechos a la intimidad, personal y familiar, así como a la imagen e identidad;

2) Constitucionalizar el derecho a la autodeterminación informativa abriría las puertas a que los ciudadanos puedan orquestar el destino de sus datos personales;

3) Los ciudadanos ignoran los peligros que acechan al revelar sus datos personales en bancos públicos o privados de información.

3.1.2. Antecedentes nacionales

Linares (2019), en su disertación titulada “El contenido esencial del derecho fundamental a la autodeterminación informativa en el Derecho Constitucional peruano”, para optar el título de abogado en la Universidad de Piura, se propuso desentrañar el alma del derecho a la autodeterminación informativa. El estudio llevado a cabo fue de naturaleza fundamental y con un enfoque descriptivo. Las conclusiones alcanzadas fueron que el derecho a la autodeterminación se erige como un derecho independiente frente a otros como la intimidad, el secreto de las comunicaciones y otros derechos, con normativa propia y contenido único, distinguible de otros.

Montes (2024), en su investigación para obtener el título de abogada en la Universidad ESAN del departamento de Lima, denominado “La vulneración del derecho a la intimidad y a la privacidad en el entorno digital en el Perú”, analizo la relación entre el derecho a la intimidad y el uso de redes sociales, su investigación cualitativa con un enfoque analítico descriptivo, concluyo que el marco jurídico nacional, prohíbe la divulgación de datos de carácter personal y familiar en un entorno digital. Sin embargo, esta salvaguarda

normativa resulta limitada al no abordar específicamente la violencia digital, en entornos como las redes sociales.

Por otro lado, Díaz (2021), en su tesis titulada “La protección constitucional del habeas data ante acumulación ilegal de información con fines de potenciales de negocio”, para optar el título de magister en derecho constitucional, en la Universidad Nacional Faustino Sánchez Carrión del departamento de Lima, se propuso medir la efectividad de la protección constitucional del habeas data ante la concentración ilícita de datos con propósitos empresariales. Para ello, creó una investigación aplicada utilizando un enfoque cualitativo. Su conclusión fue que la salvaguarda del derecho a la autodeterminación informativa es insuficiente para salvaguardar los derechos afectados por el mal manejo de la información y los datos personales; el perjuicio infligido a los afectados no se compensa y los culpables no reciben castigos con prisión efectiva.

Otro antecedente importante es la investigación de Rojas (2021), En su disertación titulada “Fundamentos para la incorporación del derecho al olvido en el sistema jurídico constitucional peruano” para obtener el título de abogado en la Universidad Cesar Vallejo Sede Trujillo, se planteó como meta primordial desentrañar si hay un abismo legal en la normativa sobre protección de datos personales que justifique la inclusión del derecho al olvido. Por tal motivo, llevó a cabo una investigación cualitativa, de enfoque descriptivo-no experimental, concluyendo que el derecho al olvido es uno de los derechos vinculados a la autonomía informativa, permitiendo la indexación y desindexación de datos personales cuando no sean de interés o relevancia para la sociedad, como consecuencia del transcurrir del tiempo.

Finalmente, Apaza (2023), para optar el grado de magister en derecho constitucional en la Universidad José Carlos Mariátegui ubicado en el departamento de Moquegua, en su reciente disertación titulada “El acceso a la información y el derecho a la intimidad personal

en la demanda de habeas data entre 1998 y 2016", buscó descubrir que las decisiones del Tribunal Constitucional peruano en 1998-2016 vinculan de manera directa la autodeterminación informativa con el derecho a la intimidad personal. Con ese propósito, llevó a cabo una investigación fundamental utilizando un enfoque cualitativo, revelando que Lima, La Libertad, Lambayeque y Arequipa concentran un 70% de las demandas de habeas data, ya sea solicitando el acceso a la información o la salvaguarda de la autodeterminación informativa.

3.1.3. Antecedentes regionales y locales

Se hizo la búsqueda local de los antecedentes de la investigación, sin embargo, no hay estudios previos al presente trabajo, por lo que no se pudo considerar ningún antecedente.

3.2 Bases teóricas

3.2.1. Derechos fundamentales

Se debe entender que estos constituyen prerrogativas inherentes a la persona, cuyo origen se sitúa en reivindicaciones históricas y posterior positivización en instrumentos nacionales e internacionales. Son derechos básicos que corresponden a todo ser humano por su condición de tal, orientados a tutelar la dignidad y asegurar condiciones de paz y justicia. Por su jerarquía normativa, gozan de mecanismos reforzados de protección en los planos legislativo, jurisdiccional e institucional.

Aunque hoy en día se reconocen los derechos fundamentales a los seres humanos, este concepto se está expandiendo para incluir también a los seres vivos de naturaleza no humana, esto en el contexto de preservar la protección ambiental, el reconocimiento de derechos en protección animal, con la finalidad de proteger y garantizar la responsabilidad social hacia la naturaleza en su forma integral.

Según el artículo 1 de la Constitución, la dignidad humana es el fin fundamental de la sociedad y del Estado. De ello deriva que los derechos vinculados directamente a la dignidad adquieren carácter fundamental. Bajo ese esquema, la positivización de derechos en el texto constitucional opera como límite a la actuación estatal y particular.

La Constitución reconoce en su Título I los derechos fundamentales de la persona, sustentados en la dignidad humana que fundamenta el catálogo del artículo 2. Asimismo, el artículo 3 establece el carácter enunciativo de dicha lista, admitiendo derechos no positivizados expresamente que se interpretan conforme a la Cuarta Disposición Final y Transitoria.

3.2.1.1. La teoría de los derechos fundamentales

Sostiene Alexy, R. (1993) que la teoría jurídica de los derechos esenciales se despliega en tres facetas: la analítica, la empírica y la normativa**.**

La dimensión analítica consiste en analizar de forma ordenada y teórica el derecho que está vigente, entre sus tareas se incluye que van desde los conceptos más básicos como norma, derecho subjetivo, libertad hasta aspectos más complejos como la creación de leyes y su relación entre una persona y cómo afecta a otros. También abarca de cómo está organizado el sistema jurídico y cómo se aplican en otras áreas con el sustento teórico del derecho. (p. 30).

La dimensión empírica puede interpretarse en dos aspectos: “En primer lugar conocer el derecho que realmente está vigente y en segundo lugar usar hechos y datos reales al momento de argumentar” (p. 30). En última instancia, la dimensión normativa conlleva la necesidad de utilizar premisas empíricas en la argumentación jurídica.

Más allá de transmitir lo que en el ámbito empírico se puede probar como derecho positivo auténtico; es la guía y la crítica de la práctica jurídica, especialmente de la jurisprudencia judicial. Para ello, la clave radica en discernir, en el contexto particular y fundamentándose en el derecho positivo vigente, la resolución adecuada. En cada caso debatido, la respuesta a esta pregunta se basa en las percepciones de quien la plantea. En gran medida, la ciencia que estudia las normas busca ofrecer una respuesta lógica a dilemas valorativos que han quedado en el limbo del material autoritario establecido. Esto enfrenta a la jurisprudencia con el dilema de la razonabilidad lógica de los veredictos de valor. (pág. 32)

3.2.1.2. Interpretación de los derechos fundamentales

Garcia (2014), en relación al fallo dictado en el expediente N°05854-2005-PA/TC, subraya que la interpretación de los derechos fundamentales trasciende las simples interpretaciones literales, teleológicas, sistemáticas e históricas, pues la interpretación de los derechos fundamentales debe fundamentarse en principios específicos, como los principios de la justicia universal:

1.- El principio pro homine, toda interpretacion debe ser en la forma en que mas le favorezca a la persona.

2.- El principio de interpretación sobre contenidos tácitos establece que la interpretación de los derechos no debe limitarse únicamente a aquellos expresamente mencionados en la Constitución, sino que también debe incluir la identificación y definición de derechos implícitos, tal como señala el artículo 3 del texto constitucional.

3.- El principio de interpretacion acorde, el cual establece que la actividad de interpretar debe tener la finalidad de armonizar, y compatibilizar el contenido de un derecho conforme

a los precedentes vinculantes y los tratados internacionales, al cual el país se encuentra adscrito.

4.- El principio de control de convencionalidad establece el deber de interpretar los derechos reconocidos en los tratados promoviendo el disfrute de estos, y sobre todo cautelarlos; y en caso de advertir que alguna norma interna desconozca el ejercicio de tales derechos, se debe velar por su expulsión del ordenamiento jurídico.

3.2.1.3. Clasificación de los derechos fundamentales

(Garcia Toma, 2014), afirma que los derechos fundamentales se clasifican en siete clasificaciones:

Por su orden cronologico de reconocimiento, dentro de estas se encuentran las de primera generacion, donde son aquellos derechos que iniciaron en el proceso de reconocimiento los llamados derechos civiles y politicos que promueven el disfrute de la libertad personal y el respeto de la autodeterminacion frente al Estado. (pág. 871)

La segunda clasificacion es por la condición del poseedor del derecho incluye privilegios como el de la personalidad, que resguarda al ser humano desde su nacimiento, permitiéndole disfrutar de su salud, libertad, conciencia y otros. En esta categoría se incluye el derecho de ciudadanía, con el propósito de asegurar que los ciudadanos colaboren activamente en cuestiones de interés público con el Estado. (pág. 875)

La tercera clasificacion es por la categoria juridica, donde se encuentran los derechos espirituales que abarcan los derechos como el de conciencia, religion, opinion y otros. Asi tambien se encuentran los derechos materiales donde se reconoce el Gozar y saborear tesoros, como el privilegio de la herencia y la posesión. (pág. 875)

La cuarta clasificacion es por su naturaleza juridica, donde se encuentran los derechos de libertad que se encuentra vinculada al libre albedrio y autodeterminacion de la persona en sociedad; los derechos de prestacion vinculada a la exigencia de lograr algo dentro de la sociedad como educacion, saud, trabajo, justicia y otros; y los derechos concurrentes que se encuentran reconocidos en otros textos legales del ordenamiento juridico. (pág. 876)

Dentro de la quinta clasificacion, según la forma en que se expresan, se diferencian los derechos explícitos que están claramente establecidos en la Constitución, los derechos implícitos que surgen del artículo 3, y los derechos asimilados que son otorgados por los tratados internacionales. (pág. 876)

En la sexta clasificacion de acuerdo a su insercion legislativa se encuentran aquellos derechos cuya raíz se encuentra consagrada en la Constitución por su reconocimiento y los derechos creados por leyes específicas. (pág. 877)

Y en la septima clasificacion se encuentran los derechos ejercidos por las circunstancias politicas, dentro de ellos se encuentran los derechos ordinarios, que se ejercen de forma regular, y los derechos extraordinarios que son ejercidos en situaciones de anormalidad politica, ejemplo el derecho a la insurgencia.” (pág. 877)

3.2.2 El derecho fundamental a la autodeterminación informativa

Sostiene Landa (2017), que la autodeterminación informativa puede entenderse de dos maneras:

1) Como un derecho subjetivo:

Su finalidad es que el titular tenga control total sobre sus datos personales almacenados en bases de datos, registros o archivos tanto públicos como privados,

permitiéndole acceder a ellos sin dificultades, solicitar su actualización, corrección o eliminación, y asegurar que cualquier cambio se realice únicamente con su consentimiento y conocimiento. (p. 76)

2) Como un principio:

Se imponen responsabilidades tanto al Estado como a las entidades privadas que recolectan o guardan los datos. En consecuencia, es imperativo instaurar entidades y estructuras administrativas y judiciales para asegurar su ejecución y resguardo contra intromisiones ajenas (derecho sancionador y salvaguarda constitucional, pilares fundamentales del derecho a la autodeterminación informativa).

Linares, (2019), señala que este derecho faculta a su titular, conocer el tratamiento de sus datos, rectificar la información personal cuando ésta sea parcial o completamente imprecisa e incompleta, o cuando se detecte algún tipo de falta, error o falsedad; eliminar la información personal cuando haya dejado de ser necesaria o relevante para el propósito para el que se recolectaron; resistirse al tratamiento de la información personal debido a una situación personal específica; y presentarse ante el Poder Judicial final y definitivamente, ante el Tribunal Constitucional (derecho de tutela).

3.2.3 Rol del Estado

La función del Estado en impulsar el progreso de la era digital y la salvaguarda de los derechos esenciales es crucial. Por un lado, debe aplicar las políticas requeridas para no obstaculizar o impedir los beneficios inherentes a ella; y por otro, debe aplicar las regulaciones apropiadas para evitar que este progreso no sea dañino para los derechos de los individuos. En definitiva, el individuo es el núcleo del Derecho y su dignidad es el objetivo supremo del Estado; por lo tanto, además de las acciones para evitar dichos ataques e imponer obligaciones a las empresas que los administran, los gobiernos deben tomar

acciones para prevenir una de las posibles causas de dichos ataques, que podrían ser los grupos terroristas. Esto lleva a tomar medidas que podrían afectar derechos básicos como expresarse libremente, acceder a la información y proteger nuestra vida privada. (Castillo, 2018, pág. 43).

3.2.4 Regulación normativa constitucional e infraconstitucional.

Según el artículo 2.6 de la Constitución señala que los bancos de datos no pueden entregar información que afecte la intimidad. Este derecho se garantiza con el hábeas data, regulado actualmente en el artículo 53 del Nuevo Código Procesal Constitucional y antes en el artículo 61 de la Ley N° 28237.

El hábeas data constituye una garantía constitucional prevista en el artículo 200 inciso 3 de la Carta Magna y desarrollada en el artículo 53 del Nuevo Código Procesal Constitucional. Esta institución tutela el derecho de toda persona a resguardar y controlar sus datos personales obrantes en bancos de datos, sean de titularidad pública o privada.

El proceso constitucional de datos, regulado en el artículo 53° del Nuevo Código Procesal Constitucional y reconocido como una garantía constitucional en el artículo 200, numeral 3 de la Constitución, permite que cualquier persona pueda proteger y supervisar todos sus datos que se encuentren registrados en bases de datos tanto públicos y privados.

(Barrera, 2004) realiza una clasificación del proceso del habeas data conforme a sus finalidades entre las cuales las define como:

- Habeas Data Informativo, donde tiene la finalidad de recabar información, ya sea para conocer qué información fue registrada, la finalidad de dicho registro, y averiguar quien obtuvo aquellos datos que se encuentran en la base de datos.

- Habeas Data Aditivo, que tiene por finalidad agregar datos al registro, ya sea para actualizarlos conforme a la realidad y al estado actual de cosas.
- Habeas Data Rectificador, tiene por finalidad modificar datos, ya sea por contener información inexacta o falsa.
- Habeas Data Reservador, tiene por finalidad garantizar la confidencialidad de la información, y que solo la persona legitimada tenga acceso a ello.
- Habeas Data Exclutorio, tiene por finalidad eliminar información ya sea por contener datos sensibles o datos que afecten el ejercicio de otros derechos.

El proceso constitucional de datos tiene como fin proteger el derecho fundamental a la autodeterminación informativa. Está regulado en el Título IV del Nuevo Código Procesal Constitucional. Inicialmente, el juez competente para estos procesos es el Juez Constitucional; sin embargo, conforme al propio Código y a la creación progresiva de juzgados especializados en materia constitucional (según la segunda disposición final del Código), en primera instancia la competencia recae en un Juez Especializado en lo Civil y, en segunda instancia, en una Sala Civil integrada por tres jueces especialistas. Para presentar la demanda, es necesario no incurrir en las causales de improcedencia señaladas en el artículo 7, agotar previamente las vías administrativas descritas en el artículo 7.4 y cumplir con los requisitos del artículo 57, que incluyen identificar la ubicación y administración de los bancos de datos, así como exponer las razones que motivan la demanda.

El sistema constitucional peruano protege el derecho fundamental a la autodeterminación informativa a través de los tratados internacionales suscritos por el país, bajo la garantía del hábeas data. A nivel infraconstitucional, este derecho está amparado por la Ley N° 29733 y su reglamento. Además, es fundamental destacar la importancia de la

jurisprudencia del Tribunal Constitucional, que establece criterios claros para la interpretación adecuada y el ejercicio de este derecho.

A nivel infraconstitucional, la Ley N.º 29733, Ley de Protección de Datos Personales, promulgada en 2011, instauró la Autoridad Nacional de Protección de Datos Personales (ANPD) como órgano rector en materia de privacidad. Adscrita al Ministerio de Justicia y Derechos Humanos, la ANPD es un ente administrativo técnico especializado con autonomía funcional. Ejerce competencias de regulación, fiscalización y sanción respecto del tratamiento de datos personales. Sus atribuciones principales comprenden:

- Garantizar la observancia de la Ley N.º 29733 y su reglamento.
- Fiscalizar que entidades públicas y privadas traten datos personales conforme a ley.
- Resolver denuncias y peticiones formuladas por titulares de datos.
- Expedir lineamientos, directivas y opiniones técnicas sobre protección de datos.
- Imponer sanciones por incumplimiento de la normativa.

Este organismo representa un pilar esencial para asegurar el balance entre el progreso digital y respeto por los derechos fundamentales, especialmente en la era de la vigilancia algorítmica, Big Data y plataformas digitales.

Esta entidad desempeña roles de administración, guía, directrices, dictamen, vigilancia y castigos. Aunque esta autoridad debe conservar el sistema, es imperativo dedicar recursos a la prevención, como informar a la comunidad sobre sus derechos de autodeterminación informativa.

En el campo de tutela de datos y entorno digital, otro hito relevante fue la instauración del Centro Nacional de Seguridad Digital (CNSD) mediante Decreto de Urgencia N.º 007-

2020. Su propósito es consolidar la confianza digital y articular la gestión de la seguridad cibernética a nivel nacional para el tratamiento seguro de la información.

Estos avances son de suma relevancia porque muestran una preocupación del Estado por el avance de la era digital y cómo hacer frente a su aprovechamiento malicioso e inclusive delictivo. Recuérdese que actualmente los datos de las personas y en general cualquier dato, puede significar desde afectaciones a derechos de intimidad, privacidad e incluso de seguridad nacional.

3.2.5 Jurisprudencia.

Ha comentado Rebollo (2023) que:

La jurisprudencia deberá tejer la narrativa y justificación de las modificaciones en los derechos, forjando una arquitectura lógica jurídica de los derechos esenciales que satisfaga las demandas emergentes y mitigue las carencias normativas, mientras facilita su aplicación y ejecución tangible. La seguridad jurídica y los mecanismos de resguardo ya existen, lo que cambian son las maneras de transgresión. Por ello, es imprescindible diseñar un ordenamiento renovado, ajustando el viejo a las demandas emergentes. Esta labor corresponde al legislador, a la jurisprudencia y a la doctrina, quienes deben armonizar las normas antiguas con las nuevas exigencias actuales. (2023, págs. 51-52).

En el ordenamiento peruano, el Tribunal Constitucional ha conceptualizado la autodeterminación informativa como el haz de facultades que permiten a toda persona controlar su información personal, sea que conste en soportes físicos, privados o digitales, a fin de impedir su utilización indebida. Esta figura jurídica se vincula al tratamiento de datos y a la tutela de la vida privada e intimidad. Su finalidad es la protección integral de la persona, comprendiendo no solo la esfera íntima, sino toda dimensión de su existencia. A

diferencia del derecho a la intimidad, que resguarda el ámbito privado, la autodeterminación informativa asegura al titular un control estricto sobre la recolección, uso y circulación de sus datos. De ese modo, confiere al titular la potestad de suprimir información sensible, impedir su propagación y oponerse a su transferencia o difusión frente a riesgos derivados del tratamiento. (STC 4739-2007-PHD/TC, fundamentos 2-4).

3.2.6 La era digital.

Diversos autores coindicen que la era digital es la cuarta revolución industrial. La humanidad se está volviendo dependiente de los medios digitales, tanto para el trabajo como en los hogares. Según estudios, el 53% de la población tiene conexión a la web. La posibilidad de acceder a la información es impresionante y se almacena en formatos digitales; los medios de comunicación han evolucionado y actualmente inclusive se puede hallar bibliotecas virtuales. (Villar Mir, 2019).

Es evidente que la emergente sociedad digital no puede ser confinada únicamente al Derecho, ya que implica una metamorfosis horizontal del tejido social, impactando a los medios de comunicación, a la economía, a cada rincón del tejido social e incluso a las bases de la organización y la política (Rebollo Delgado, 2023, pág. 52).

Así, según Pérez (2018), asistimos a lo que ha denominado “Los derechos humanos en la tercera era: los privilegios de la era digital”, entre los cuales podemos enumerar los siguientes (pp. 144-155):

- Los derechos vinculados a la protección de la calidad de vida, y salud.
- Los derechos asociados a las herramientas digitales para informar y comunicar.
- Los derechos derivados de la bioética y la biotecnología.

Sin embargo, la facilidad con la que se carga y descarga la información a nivel mundial genera serios peligros. Un claro ejemplo de estos peligros es lo que pasó en EE. UU. en el año 2017, donde Facebook admitió que 126 millones de usuarios habrían sido influidos por supuestos agentes rusos en un contexto electoral. (Villar Mir, 2019).

De igual manera, la manipulación de la información, la información inexacta o la falsificación de identidad es uno de los problemas de tal accesibilidad. Una vez que se presentan, sin duda afectan enormemente a las víctimas y el derecho debe tener las herramientas adecuadas para prevenir mayores daños, sancionando a los responsables, ya sea por dolo o culpa inexcusable.

Bajo ese sentido, como señala Pérez (2018), los derechos humanos de tercera generación cumplen el papel de establecer un enlace entre la realidad científica tecnológica actual y sus expectativas. Por lo tanto, constituyen la respuesta más apropiada y eficiente a los desafíos emergentes de la tecnociencia. Ya que, (...) buscan aprovechar al máximo la potencialidad de los avances científicos y tecnológicos y, simultáneamente, instauran un sistema de garantías para evitar que dichos avances se realicen a expensas de las libertades. Los derechos humanos de la tercera generación tienen una doble responsabilidad: utilizar al máximo los progresos de la tecnociencia para mejorar las condiciones de vida de las personas y prevenir el deterioro o contaminación tecnológica de las libertades (liberties pollution) (pp. 149-150).

En nuestro país, la autodeterminación informativa es el derecho y poder de decisión que tiene cada persona de conocer qué pasa con sus datos personales, en papel o en internet, para que no sean mal utilizados o con fines distintos a los inicialmente otorgados. Está ligado a la protección de la vida privada, pero es más amplio: cuida toda la vida de la persona, no

solo lo íntimo. Mientras la intimidad protege lo privado, la autodeterminación informativa le da a cada uno control total sobre cómo se recogen, usan y comparten sus datos.

Actualmente, el Gobierno viene implementando políticas públicas de gobierno digital orientadas a promocionar la digitalización en sus servicios. Dentro de estas políticas tenemos:

El Decreto Legislativo N° 1412, conocido como la "Ley de Gobierno Digital" y publicado en 2018, el cual fue creado con el objetivo de fomentar la digitalización en la prestación de servicios públicos. Su ámbito de aplicación abarca:

Artículo 2.- (…) se aplica a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N.º 27444, Ley del Procedimiento Administrativo General. Sus regulaciones también alcanzan a las personas jurídicas o naturales que, por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros. 2.2. En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable. (Poder Ejecutivo, 2018, pág. 1).

El Decreto de Urgencia N°006-2020 "Creación del sistema de transformación digital", esta ley surgió con la finalidad de modernizar la administración pública, promoviendo la digitalización en la prestación de servicios por parte del Estado, brindando servicios digitales de calidad. (Poder Ejecutivo, 2020).

El Decreto de Urgencia N.º 007-2020 tiene como objetivo principal asegurar la confianza de las personas en sus interacciones con servicios digitales, tanto de entidades

públicas como privadas. Esto significa que dichas interacciones digitales deben ser seguras y transparentes, permitiendo a los usuarios tener plena confianza en el uso de las tecnologías digitales. Además, su artículo 7 establece la creación del Centro Nacional de Seguridad Digital, cuyo propósito es supervisar y fortalecer la confianza digital en la prestación de servicios de la administración pública. (Poder Ejecutivo, 2020).

El Decreto Supremo N° 029-2021-PCM establece el reglamento del Decreto Legislativo N° 1412, cuyo objetivo es coordinar y fomentar el proceso de transformación digital en las entidades del sector público. (Poder Ejecutivo, 2021).

El decreto Supremo N°85-2023-PCM, aprueba la Política Nacional de Transformación Digital al 2030, alineado al Decreto de Urgencia N°006-2020, bajo esta política se reconoce que la transformación digital es un instrumento estratégico para el desarrollo nacional, mejorando la prestación de servicios estatales, y fomentan iniciativas y a la sociedad en general adaptarse a la transformación digital. (Presidencia del Consejo de Ministros, 2023).

La ley N°31814 “Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país” publicada el 5 de julio del 2023; esta ley busca reconocer y utilizar la inteligencia artificial a fin de mejorar los servicios públicos y privados. (Congreso de la República, 2023).

La conexión entre la era digital y el derecho fundamental a la autodeterminación informativa se fundamenta en la dignidad humana; por ello, en el reconocimiento y resguardo de los derechos debe priorizarse la protección del individuo en cuanto a su dignidad, garantizando así la libertad individual frente a las nuevas tecnologías de información. (Sarrión, 2023).

3.2.7 Casos emblemáticos.

A nivel internacional

1) Caso Cambridge Analytica

El caso evidenció la administracion ilícita de datos personales con fines electorales, donde Facebook facilitó a la consultora Cambridge Analytica información de usuarios para diseñar campañas electorales personalizadas.

En 2014, Cambridge Analytica obtuvo de Facebook datos de 87 millones de usuarios sin consentimiento. La información comprendía mensajes privados, interacciones como "Me gusta", preferencias electorales y otros datos con el fin de influenciar a los votantes en el proceso electoral. Dicha data se utilizó en las elecciones presidenciales de Estados Unidos de 2016 y en el referéndum del Brexit. A raíz de ello, Facebook Inc. fue citada ante el Congreso de EE. UU. y sancionada con una multa de cinco mil millones de dólares por el tratamiento indebido de datos personales.(Vercelli, 2018).

2) Caso Equifax

Equifax es una empresa transnacional que tiene como objetivo de negocio brindar información sobre los riesgos crediticios de una persona para acceder a un crédito financiero.

En 2017 esta empresa fue víctima de un ciberataque de filtración a sus sistemas de información, y se sustrajeron datos de las personas como números de tarjetas de crédito, licencias de manejo, datos de identificación, direcciones, y otros, evidenciándose la poca seguridad y el alto riesgo de una empresa transnacional que administra datos personales.(Polanco, 2020).

3) Snowden

Edward Snowden, fue un extrabajador de la NSA, y en el año 2013 revelo que la NSA a través de sistemas electrónicos realizaba una vigilancia masiva a nivel de todo el mundo denominándolo proyecto “MUSCULAR” (proyecto dirigido por el Estado británico y los Estados Unidos, con la finalidad vigilar a los usuarios en internet, con el fundamento de la lucha contra el terrorismo), interceptando y procesando correos electrónicos, llamadas y otros, de millones de ciudadanos a nivel mundial. Esta vigilancia fue facilitada debido a que los sitios webs, servicios de mensajerías y otros, no ofrecían sistemas de ciberseguridad a través de encriptación a los datos que se encontraban bajo su administración, este hecho generó que empresas como Google, Microsoft, y otros, asuman conductas responsables cifrando de extremo a extremo los datos de los usuarios, conociendo a esta última como “seguridad estándar”. Los principales diarios de comunicación del mundo como The Guardian y otros, fueron quienes principalmente empezaron a publicar las declaraciones de Snowden, exponiendo que empresas como Verizon recolectaban datos personales generando informes para la NSA (Serrano, 2021).

A nivel nacional

1) Caso Chuponeo.

La interceptación a las llamadas telefónicas por parte de privados, e incluso por parte del Estado a ciudadanos, y con mayor razón a altos funcionarios como jueces, fiscales y figuras políticas como expresidentes en nuestro país es una práctica que ha sacudido y revelado los casos de corrupción más escandalosa en la historia de la Republica del Perú, como el caso Petro audios, el caso Hinostroza y otros. Sin embargo el objetivo de esta investigación no es concentrarse en los hechos delictivos suscitados, sino, en la utilización de la interceptación de las llamadas telefónicas, de estos ciudadanos peruanos, si bien nuestro ordenamiento jurídico prevé limitaciones al derecho a la privacidad, como la interceptación de las comunicaciones, este alcance legal se hace efectivo previa autorización

judicial, mediante resolución judicial; sin embargo, en la actualidad se está dando el "chuponeo" en términos de basilecto, sin previa autorización, y motivado por privados que al margen de la ley vulneran la privacidad de las personas. (RPP, 2017).

2) Caso Juan Mejía Seminario

Juan Mejía Seminario demandó a través de una demanda de amparo al propietario de Facebook, ya que, en el año 2021, la red social suspendió temporalmente su cuenta debido a que este compartió una noticia sobre la pandemia del 2020. Tras aplicar sus herramientas, la red social calificó el contenido como información falsa. Por ende, procedió a suspender temporalmente su cuenta personal por el termino de 30 días, porque de acuerdo a la plataforma, este actuar de dicho usuario vulneraba las normas de la comunidad de "Facebook". (Ingunza, 2022).

Lo suscitado refleja que Juan Seminario en el uso de su red social que cabe aclarar le sirve para desenvolverse en el mundo virtual ya sea para comunicarse y ejercer su libertad de expresión, también fue un usuario que simplemente posteó una noticia que ya circulaba en la red social, es decir, él no fue el propietario de dicha noticia falsa.

Aquí cabe preguntarnos: ¿qué se considera falso y que criterios tiene Facebook para determinar la verdad? A fin de determinar que algo es verdad, tiene que estar sustentado en evidencias, la lógica, y en realidades objetivas; la red social utiliza el "machine learning" a fin de validar datos, lo cierto es que esta validación no implicaría llegar a la conclusión de la veracidad de la información que circula en la red, puesto que en esta red circulan datos como opiniones, predicciones personales, posiciones personales frente a noticias de trascendencia mundial, nacional, personal, religioso y otros, y si bien los usuarios estamos expuestos a consumir toda clase de información en las redes, somos los únicos que en ejercicio de nuestra libertad de autodeterminación informativa, deberíamos decidir con que información estamos de acuerdo y con qué otras no, y esto no supone un sometimiento al

test de veracidad, lo cual no debería implicar llegar a limites como la suspensión de la cuenta de un usuario, por el posteo de una información “supuestamente falsa”, cuando fue Facebook que expuso al usuario frente a tal noticia.

3.3 Definición de términos

a) Autodeterminación informativa

Este derecho se forja a partir del concepto de intimidad, entendido como "el reconocimiento del ser humano de un área de vida personal única y exclusiva, de una actividad íntima y única que puede cerrar la puerta a otros”. (Pérez, et al, 2019, p. 12).

Por este derecho, se garantiza que toda persona pueda controlar su información que se encuentre almacenada en bases de datos, ya sea para corregir, actualizar, o incluso suprimir información que no deba encontrarse registrada.

b) Contenido esencial del derecho fundamental

Comenta Linares (2019), el núcleo esencial es “el arsenal de poderes que transforman al derecho en ese derecho y no en un derecho diferente”, y se encuentra sustentado sobre la “dignidad humana” (p. 123).

Para Abad (1992), el contenido esencial se refiere a aquellos elementos esenciales que lo hacen reconocible y que impiden su metamorfosis en algo distinto; para determinar su esencia, no basta con recurrir a la Constitución, sino que es necesario explorar otros conceptos jurídicos y las convicciones comunes entre los juristas. “Se trata de un valor inmutable, inalterable independientemente de las circunstancias que se mencionen”, ya que “cada derecho fundamental posee un contenido esencial único y distintivo, y su alcance no puede ser generalizado” (p. 10).

c) Constitución

De acuerdo con el neoconstitucionalismo.

Es un documento legal, generalmente escrito, que reina sobre todas las demás regulaciones del sistema jurídico estatal y, por ende, determina la validez tanto formal como material de todas las leyes secundarias del país en el que opera. En su esencia, es una estructura normativa sólida que alberga un vasto repertorio de derechos (humanos o fundamentales, según cada época y perspectiva teórica) estructurados con fórmulas abstractas y abiertas, y que actúa como el núcleo esencial del documento y, a través de él, del ordenamiento en su totalidad. Este pilar constituye la columna vertebral del documento y, a través de él, del ordenamiento en su totalidad. (Salazar, 2015, p. 1940).

d) Derecho fundamental a la autodeterminación informativa

A decir de Landa (2017), el derecho a la autodeterminación informativa.

Es derecho y responsabilidad del titular administrar sus datos recopilados, registrados en bases de datos, archivos o registros, tanto públicos o privados, a fin de garantizar que la información no sea modificada en su perjuicio, ni sea transferida o vendida sin su autorización y conocimiento previo. (pág. 75).

e) Sistema normativo

Un conjunto de enunciados tales que entre sus consecuencias hay enunciados que correlacionan casos con soluciones, de lo que se sigue que todo conjunto normativo que contiene todas sus consecuencias es un sistema normativo.

Expresado de otra forma, un sistema de enunciados que tiene consecuencias normativas se denomina sistema normativo y debe contener como criterio a un conjunto de enunciados en cuyas consecuencias existe, por lo menos, alguna consecuencia normativa. (Álvarez, 2021, p. 11).

f) Titularidad de derechos

Según Contreras (2017), describe a la titularidad como “un estatus normativo o condición legal en la que se identifica un individuo que se beneficia con la protección del derecho, equidad o libertad que un sistema legal considera como derecho esencial.” (p. 120).

g) Poderes del Estado

Su definición proviene de la doctrina liberal del siglo XIX, específicamente de Montesquieu, quien en su obra jurídica “El espíritu de las leyes”, concluyo que los poderes del Estado son tres: el Legislativo (encargado de promulgar las normas), el Ejecutivo (encargado de aplicar las políticas y normas) y el Judicial, el que administra justicia concreta (Ugarte, 2015).

h) Sistema constitucional peruano

Es la estructura y organización del Estado peruano, teniendo como base la Constitución Política de 1993, la cual es la ley fundamental que orienta y dirige la estructura normativa infraconstitucional.

El Sistema Constitucional garantiza que se respeten los derechos fundamentales y se ajusten a lo que la Constitución establece, por ende, establece los derechos y deberes de las personas y establece los límites del actuar de los poderes públicos.

i) Habeas Data

La Constitución, en su artículo 200, numeral 3, junto con el artículo 57 del Nuevo Código Procesal Constitucional, reconoce esta garantía con dos objetivos principales: primero, asegurar que las personas puedan acceder a la información que se encuentra en bases de datos públicos y privados bajo administración; y segundo, proteger el derecho a la autodeterminación informativa, que implica que cada individuo tenga control sobre cómo se utiliza, almacena y comparte su información personal, decidiendo qué datos se guardan, quién puede acceder, modificar o eliminar esa información, y evitando que se use sin su consentimiento.

El tribunal Constitucional ha señalado que este derecho se encuentra arraigado en el inciso 6) del artículo 2° de la Constitución y es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen. (N°1797-2002-AA/TC, 2002, pág. 2).

IV. Metodología

4.1. Tipo y nivel de investigación

4.1.1 Tipo de investigación

Según Carrasco (2019) indica que el tipo de investigación básica "únicamente aspira a expandir y abordar con mayor profundidad la sabiduría científica existente sobre la realidad. Su meta de investigación son los postulados científicos, las cuales examina para mejorar sus contenidos" (p.43). Esta investigación pretende analizar el derecho fundamental a la autodeterminación informativa en el entorno digital, a fin de generar conocimiento útil para la ciudadanía.

4.1.2 Nivel de investigación

Esta investigación tiene un enfoque analítico-descriptivo, ya que se dedica a explorar un tema poco abordado en el Perú como la protección y el ejercicio del derecho fundamental a la autodeterminación informativa ante los retos que plantea la era digital, además de examinar las conexiones entre sus aspectos normativos, doctrinales y jurisprudenciales dentro del sistema constitucional peruano. Este nivel de investigación permite abordar un tema complejo y en permanente cambio, como el cuidado de los datos de las personas en el mundo digital, ya que ayuda a detectar deficiencias legales, retos y áreas de mejora en la protección constitucional del derecho a decidir sobre la propia información, sin necesidad de manipular categorías ni realizar experimentos.

De acuerdo con Hernández, et al. (2014), se considera adecuada la investigación analítico-descriptiva, ya que permite describir con precisión las características, hechos o fenómenos de un objeto de estudio, y por otro lado analizar las relaciones de los elementos que componen dicho fenómeno. Así, este marco metodológico permitirá analizar y comprender cómo se configura este derecho en la práctica constitucional peruana, revelando

tensiones entre innovación tecnológica, derechos fundamentales y marcos normativos vigentes.

4.2 Ámbito temporal y espacial

Este estudio examina la aplicación del ordenamiento jurídico peruano en materia de protección de datos personales, ante desafíos de la era digital. Para ello, se realizó entrevistas a magistrados del Distrito Judicial de Apurímac con competencia en materia constitucional, así como a ingenieros informáticos de los Distritos Judiciales de Apurímac y Cusco, con el objetivo de recoger criterios técnicos especializados en seguridad de la información.

El estudio comprende el periodo de años 2020-2024 y se enfoca a la tutela del derecho a la autodeterminación informativa

Al tratarse de un estudio cualitativo de alcance nacional, la selección de distritos judiciales no afecta la validez de los resultados, pues la normativa está vigente en todas las regiones de nuestro país.

4.3 La población y muestra

Al ser una investigación con enfoque cualitativo, la población y la muestra estuvo conformada por los representantes del órgano jurisdiccional del Distrito Judicial de Apurímac conocedores del tema de investigación, que son pocos debido a ser una materia reciente como la “Era Digital”, donde la tecnología impacta directamente en la protección de datos personales, siendo:

- 04 jueces con especialidad en Derecho Civil o Constitucional en razón que son los representantes del órgano jurisdiccional que resuelven procesos de Habeas data, en primera y segunda instancia.

- 03 ingenieros en informática del Poder Judicial, con el propósito de examinar el alcance del derecho a la autodeterminación informativa desde su perspectiva profesional,

así como para entender la gestión y protección de datos en las Cortes Superiores de Justicia de Apurímac y Cusco.

Y, los documentos normativos como:

- Constitución Política del Perú.
- Nuevo Código Procesal Constitucional.
- Ley de Protección de datos personales.
- Nuevo Reglamento de la Ley de Protección de Datos Personales.
- Jurisprudencia emitida por el Tribunal Constitucional.
- Leyes que regulan la era digital.

El muestro fue no probabilístico.

4.4 Instrumentos

4.4.1. Técnica de recolección de la información

4.4.1.1 Técnica de la entrevista:

Es una técnica esencial en la investigación cualitativa, ya que permite obtener percepciones profundas y contextualizadas de actores clave sobre fenómenos sociales y jurídicos. Respecto de la investigación sobre la autodeterminación informativa en el ámbito digital nacional, la técnica empleada permite recabar las apreciaciones de juristas especializados en derecho constitucional, autoridades competentes y profesionales en seguridad de la información.

Según Taylor y Bogdán (1987), la entrevista cualitativa facilita la comprensión del significado que las personas atribuyen a sus experiencias. Así, se accede a perspectivas

valiosas sobre la eficacia normativa y los desafíos digitales que enfrenta este derecho fundamental.

4.4.1.2 Análisis documental:

Es una técnica cualitativa que permite examinar críticamente textos jurídicos, doctrinales y normativos para identificar patrones, significados y transformaciones en un contexto determinado. En el análisis del derecho a la autodeterminación informativa en el Perú, este método permite realizar una revisión ordenada de normativas, fallos judiciales y documentos oficiales vinculados a la protección de datos personales. Según Bowen (2009), el análisis documental permite contextualizar y triangular información con otras técnicas cualitativas. Así, se comprende cómo el sistema constitucional peruano ha enfrentado los retos de la era digital.

4.4.2. Instrumento de recolección de información

4.4.2.1 Guía de entrevista estructurada:

Es un instrumento diseñado para aplicar entrevistas con preguntas previamente definidas. En investigaciones sobre derechos digitales, su uso facilita la comparación de respuestas entre distintos actores, como jueces y servidores públicos (Ingenieros informáticos).

4.4.2.2 Ficha de análisis documental:

La ficha de análisis documental es una herramienta metodológica relevante en la investigación cualitativa, ya que permite organizar y examinar críticamente fuentes jurídicas, doctrinales y normativas. En el estudio del derecho a la autodeterminación informativa en el Perú (2020–2024), esta técnica facilita el análisis sistemático de la

Constitución, jurisprudencia del Tribunal Constitucional, leyes sobre protección de datos, y el marco normativo digital.

Según Flick (2015), esta técnica no solo describe, sino que interpreta fenómenos complejos. Su uso permite comprender cómo el sistema jurídico peruano ha respondido ante los desafíos digitales. Así, se construye una base sólida para la reflexión crítica y contextual del derecho fundamental investigado.

4.5 Procedimientos

El proceso de recopilación de datos tuvo lugar a través de entrevistas cualitativas, siguiendo una serie de fases meticulosamente organizadas para asegurar la validez de la información recabada. Primero, se reconoce y elige a los participantes, después se inicia el contacto para dar a conocer los propósitos de la investigación y conseguir el consentimiento informado, garantizando que los participantes entiendan sus derechos y la privacidad de sus respuestas. En la entrevista, el investigador emplea un instrumento ordenado que ayuda a analizar a profundidad lo que piensan las personas, conforme a sus vivencias de los participantes.

Las entrevistas se realizan con la garantía de confidencialidad para obtener respuestas honestas. Con consentimiento previo, se transcriben para analizarlas y detectar el punto central de la investigación.

4.6 Análisis de datos

Los datos cualitativos de las entrevistas se analizan de forma sistemática y rigurosa. Tras la recolección, se interpretan las respuestas para identificar experiencias y opiniones de los participantes sobre hábeas data, y protección de datos personales.

Previamente este procedimiento se enriquece con la contribución de los antecedentes, que tiene como objetivo fusionar y perfeccionar las categorías en ideas fundamentales que

expliquen cómo la autodeterminación informativa permite garantizar el respeto de los derechos fundamentales consagrados en la Constitución.

4.7 Consideraciones éticas

El estudio garantizó la reserva de los datos, con respeto a la autonomía de los participantes. Se aplicó el consentimiento informado previo y se cumplieron las directrices institucionales y las normas APA séptima edición. Se reconoció la autoría intelectual mediante el citado correcto de fuentes.

V. Resultados y discusión

5.1. Resultados de la entrevista

En esta parte se hace la transcripción de las entrevistas a los jueces civiles o constitucionales y a los ingenieros del área de soporte informática del Poder de Judicial de Apurímac y Cusco sobre el tema de investigación:

5.1.1. Transcripción de las entrevistas a los jueces civiles o constitucionales y a los ingenieros del área de soporte informática del poder de judicial de Apurímac y Cusco.

Donde:

- Juez 1: Juez de primera instancia
- Juez 2: Juez de primera instancia
- Juez 3: Juez de segunda instancia
- Juez 4: Juez de segunda instancia

***Tabla 2**: Cuadro de transcripción de respuestas de entrevistados (Jueces)*

PREGUNTA JUECES CIVILES O CONSTITUCIONALES			**RESPUESTA**
Objetivo general: Analizar la protección legal del derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano.	**Juez 1**	¿Cómo analiza e interpreta usted el derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano?	Es conocido como el derecho a la protección de datos personales, con este derecho se permite a los ciudadanos controlar la información personal que se recopila, almacena y utiliza sobre ellos.
	Juez 2		Por este derecho se busca proteger la intimidad, imagen, identidad personal y familiar frente al uso y manipulación de datos a través de medios electrónicos.
	Juez 3		Considero que el derecho a la autodeterminación informativa implica la facultad de las personas para controlar y decidir sobre la recopilación, almacenamiento, uso y difusión de sus datos personales. Sin embargo, es fundamental reconocer que la era digital plantea nuevos desafíos y riesgos para la protección de la autodeterminación informativa, como la vigilancia masiva, la minería de datos y la difusión de información personal sin consentimiento.
	Juez 4		El derecho a la autodeterminación informativa se encuentra reconocido en la Constitución, la era digital ha generado nuevos desafíos para la protección de este derecho, ya que la información personal se encuentra cada vez más expuesta y vulnerable a la recolección, procesamiento y difusión sin control.

	Juez 1	¿Cuáles han sido los principales desafíos que ha enfrentado el sistema judicial en la protección de este derecho frente al avance de la era digital?	La rápida evolución de las tecnologías de la información y la comunicación ha superado la capacidad del sistema judicial para adaptarse y regular adecuadamente el uso de datos personales.
	Juez 2		La vulnerabilidad de datos personales ya que los servicios informáticos, públicos o privados, suministran información que afecta la intimidad personal o familiar.
	Juez 3		Los desafíos que ha enfrentado serian la velocidad de los avances tecnológicos y el cómo la legislación peruana en materia de protección no puede seguir su paso. También tenemos la falta de capacitación a jueces y funcionarios judiciales para abordar completamente los temas relacionados con la protección de datos personales en esta era digital.
	Juez 4		Existe una falta de regulación clara y actualizada sobre la protección de datos personales, frente al avance de la era digital. Así también, existe conflictos de derechos, entre la autodeterminación informativa y otros derechos, como la libertad de expresión y la libertad de información.
	Juez 1	¿Considera que la normativa vigente es suficiente para garantizar la autodeterminación informativa en la era digital, o se requieren reformas?	No es suficiente, ya que la normativa actual frente a la inteligencia artificial y el Big Data han transformado la manera en la que se recopilan datos y nuestra normativa no está completamente equipada para abordar los riesgos asociados a estas tecnologías. Desde mi perspectiva me parece insuficiente, sobre todo en materia procesal, ya que en algunos casos se tiene que emplazar a bancos de datos internacionales que tienen su domicilio en el extranjero, lo cual hace que el proceso de habeas data sea más largo, lo cual desnaturaliza la naturaleza de un proceso constitucional que se garantiza por ser sumario y urgente, y más aún cuando se trata de supresión de datos que se encuentran en el internet, mientras el proceso siga en trámite, los datos se encuentran allí y se difunden a gran velocidad, lo cual podría agravar la situación del justiciable en relación a otros derechos. Así también, en el caso de ejecución de sentencias, estas empresas podrían no ejecutar la sentencia alegando la falta de jurisdicción.
	Juez 2		No es suficiente, y se requieren reformas para abordar los desafíos específicos del entorno digital, ya que existen amenazas de la inteligencia artificial, por la falta de control de la inteligencia artificial para transformar imágenes e información. Así también, se deben regular las redes sociales en relación a la protección de la información en línea.
	Juez 3		A pesar de la normativa vigente es un buen punto de partida, se requieren reformas y actualización para garantizar la autodeterminación informativa en la era digital. Un claro ejemplo de reforma seria el fortalecimiento de las medidas de seguridad y protección de datos personales, así como una mayor cooperación internacional para abordar los desafíos trans fronterizos en la protección de datos personales.
	Juez 4		No es suficiente, ya que se requieren reformas como actualizar la legislación para abordar los desafíos de la era digital, como la protección de datos personales en línea y la regulación de las redes sociales.

			También, se requieren mecanismos efectivos para la protección de datos sensibles y la prevención de la discriminación en línea.
Objetivo específico 1: Describir de qué manera se protegen los datos personales generales frente a la era digital en el sistema constitucional peruano.	**Juez 1**	¿Cómo está regulado el derecho fundamental a la autodeterminación informativa en el sistema constitucional peruano?	Está regulado en la Constitución articulo 2 numeral 6, la Ley de Protección de Datos Personales y el Código Procesal Constitucional en el Habeas Data.
	Juez 2		A través del Artículo 2 inciso 6 de la Constitución y a través del Habeas Data, que permite a las personas acceder a la justicia para conocer, actualizar, suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados en banco de datos.
	Juez 3		El derecho a la autodeterminación informativa en el sistema constitucional peruano esta regulado por una combinación de normas constitucionales, leyes, reglamentos y jurisprudencia y doctrina, que buscan proteger la privacidad y la autodeterminación de los individuos en el ámbito digital.
	Juez 4		Se encuentra regulado en la Constitución articulo 2 numeral 6 y protegido con la garantía constitucional del habeas data. Así también, con la ley de protección de datos personales.
	Juez 1	¿Qué aspectos normativos han sido objeto de mayor debate o controversia en los últimos años?	El derecho al olvido, su aplicación práctica ha sido limitada y enfrenta resistencia. El consentimiento informado, especialmente en el contexto de tecnologías emergentes, como la inteligencia artificial y el Big data. Se cuestiona si las personas realmente comprenden el uso de sus datos personales.
	Juez 2		El derecho al olvido, el Tribunal Constitucional peruano se ha pronunciado sobre el derecho al olvido, que garantiza la eliminación, supresión o retiro de información relacionado con datos personales usualmente vinculados al nombre de la persona
	Juez 3		Serian el equilibrio entre el derecho a la información y el derecho a la privacidad ya que pueden llegar a entrar en conflicto. Reitero el que se debe actualizar la normativa, la necesidad de actualizar la normativa para abordar los nuevos desafíos planteados por la era digital ha sido objeto de debate y controversia.
	Juez 4		La ley de protección de datos personales de manera sui generis, especialmente en relación con la protección a la privacidad e intimidad, frente a la autodeterminación informativo en la era digital.
	Juez 1	¿Existen vacíos normativos o conflictos legales en la regulación de este derecho?	Si, existen varios vacíos normativos, la normativa actual no aborda adecuadamente los desafíos que presentan las tecnologías emergentes como la inteligencia artificial y el Big Data. En un aspecto procesal se tiene que el proceso del habeas data debería garantizar el derecho a la autodeterminación informativa, pero en la realidad no resulta ser un proceso célere.
	Juez 2		Si, como determinar si las personas jurídicas pueden ser titulares de datos personales. Protección en redes sociales, no está claro si el derecho a la autodeterminación informativa se aplica en la actividad de los usuarios de redes sociales, especialmente en lo que respecta a la publicación de datos de terceros.

			En materia procesal el proceso de habeas data, debería establecer algunos mecanismos como la notificación electrónica validada solo en el caso de emplazamiento a empresas internacionales, a fin de que el proceso pueda ser célere, y en el tema de ejecución de resoluciones se deberían establecerse mecanismos de cooperación internacional célere.
	Juez 3		Si, existen vacíos normativos y conflictos legales, tenemos la falta de regulación específica sobre el uso de datos personales en el ámbito digital y la insuficiente regulación sobre la vigilancia y el acceso a la información.
	Juez 4		Aunque la ley de protección de datos personales establece principios y garantías para la protección de datos personales, no aborda específicamente los desafíos de la era digital, y ello es a nivel infraconstitucional. Lo correcto debería ser que el proceso del habeas data, proteja adecuadamente el derecho a la autodeterminación informativa, sin embargo, este proceso constitucional no es célere, por ende, el proceso constitucional debería regular aspectos como el emplazamiento a empresas internacionales, donde se garantice el debido proceso y sobre todo el cumplimiento de plazos procesales conforme a ley.
Objetivo específico 2: Explicar de qué manera se encuentran protegidos los datos sensibles frente a la era digital en el sistema constitucional peruano.	**Juez 1**	¿Cómo se regula la era digital en el sistema constitucional peruano?	Está regulada en varias normas, desde la Constitución Artículo 2 inciso 6, la Ley de Protección de Datos Personales y las Políticas de Transformación digital.
	Juez 2		A través, de la ley de gobierno digital, que establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, los servicios digitales, la arquitectura digital, la interoperabilidad, la seguridad digital y los datos. Su objetivo es que las entidades estatales se integren las tecnologías digitales para prestar servicios en condiciones seguras, confiables y transparentes.
	Juez 3		La regulación de la era digital en el sistema constitucional peruano se encuentra dispersa en varias normas y principios constitucionales y legales y se enfoca en proteger los derechos fundamentales y garantizar la transparencia y la seguridad en la gestión de la información.
	Juez 4		No existe ley que regule la era digital, ya que se encuentra en proceso de desarrollo y evolución. Sin embargo, la constitución protege algunos derechos como la intimidad, el honor, la privacidad, la libertad de información y expresión, que se pueden interpretar en el contexto de la era digital.
	Juez 1	¿De qué manera ha influido la transformación digital en la interpretación y aplicación de los derechos fundamentales en el Perú?	La digitalización ha aumentado la cantidad de datos personales que se recopilan y procesan, lo que ha llevado a una mayor atención y regulación en torno a la protección de estos datos.
	Juez 2		La transformación digital, ha impactado en la identificación de los derechos digitales que garantizan la seguridad y la libertad en el entorno virtual, incluyendo la libertad de expresión, neutralidad en internet, privacidad y protección de datos, derecho al anonimato, derecho al olvido, propiedad intelectual, derecho a compartir conocimiento, acceso a la información pública, acceso a la cultura y conocimiento y uso recreativo de la tecnología.
	Juez 3		La influencia ha sido significativa para esta influencia ha sido tanto positiva como negativa.

			En lo positivo tenemos la ampliación del acceso a la información la facilitación de la participación ciudadana y la mejora en la trasparencia y rendición de cuentas. Con respecto a lo negativo serían los riesgos para la privacidad y protección de datos y desafíos para la libertad de expresión.
	Juez 4		Ha traído beneficios como ha facilitado el acceso a la información lo que ha permitido a los ciudadanos ejercer su derecho a la libertad de información y expresión. Pero ha traído desafíos en relación con la privacidad y la protección de datos personales, lo que ha llevado a una mayor vulnerabilidad a la vigilancia y el control.
	Juez 1	¿Cómo se han abordado temas como la protección de datos personales y la privacidad en este contexto?	Se abordaron desde distintas normativas. Sin embargo, el habeas data es la única garantía constitucional que permite a los ciudadanos solicitar la protección de sus datos personales y exigir la corrección a la eliminación de información incorrecta o no autorizada.
	Juez 2		A través de la ley de protección de datos personales ley 29733, a través del reglamento de la ley de protección de datos personales y a través de la entidad la autoridad nacional de protección de datos personales, que fiscaliza el cumplimiento de la ley de protección de datos y su reglamento.
	Juez 3		A través de la Ley de Protección de Datos Personales, Ley 29733, y el Reglamento de la Ley de Protección de Datos Personales.
	Juez 4		Se abordaron a través de la ley de protección de datos personales y el reglamento general de protección de datos. Sin embargo, el MINJUS ha elaborado campañas de conciencia para educar sobre la protección de datos personales y la privacidad.
Objetivo específico 3: Determinar cómo se regula el consentimiento informado frente a la era digital en el sistema constitucional peruano.	**Juez 1**	¿Qué mecanismos pueden adoptarse para proteger el derecho a la autodeterminación informativa frente a la era digital?	La actualización de la legislación, ya que se tienen que adaptar leyes existentes para abordar los desafíos de las nuevas tecnologías, como la inteligencia artificial y el Big Data. Fortalecimiento del proceso del Habeas Data, para mejorar el acceso y eficacia del proceso del Habeas Data.
	Juez 2		La designación de un oficial de datos personales, a fin de que en las entidades públicas o privadas y en aquellas que manejen grandes volúmenes de datos sensibles afecten a un gran número de personas, esto a fin de tomar medidas preventivas en la filtración de información.
	Juez 3		Se podrían adoptar los mecanismos legales y regulatorios, las tecnologías, los educativos y de conciencia y sobre todo los mecanismos de supervisión y control.
	Juez 4		Establecer regulaciones para la recolección y uso de datos personales, incluyendo la obtención de consentimiento informado
	Juez 1	¿Cómo garantiza el estado mediante el Poder Judicial el equilibrio entre la innovación tecnológica y la protección de los derechos	A través del marco legal y normativo, y la jurisprudencia donde el Tribunal Constitucional, ha emitido diversas sentencias que interpretan y desarrollan el alcance de los derechos fundamentales en el contexto de la era digital.
	Juez 2		A través de la implementación de las tecnologías de forma progresiva, así también algunos magistrados estamos utilizando la inteligencia artificial a fin de obtener información precisa. Sin embargo, resulta analizar siempre las implicancias éticas y legales.
	Juez 3		A través de la interpretación y aplicación de la ley.

	Juez 4	fundamentales ?	Garantizar el equilibrio a través de la interpretación y aplicación de la ley, la protección de los derechos fundamentales y la promoción de innovación tecnológica, siempre en cuando no se vulneren los derechos fundamentales.
	Juez 1	¿Cómo puede fomentarse una cultura de protección de datos y autodetermina ción informativa en la sociedad peruana?	A través del fortalecimiento de la legislación, como actualizar y fortalecer las leyes existentes para abordar los desafíos de las nuevas tecnologías como la inteligencia artificial y el Big Data.Que se impongan sanciones más severas para las entidades que no cumplen con las normativas de protección de datos personales.
	Juez 2		Realizando campañas educativas digitales dirigidas a ciudadanos y empresas sobre la importancia de la protección de datos personales y los derechos que les asisten. Esto incluye como ejercer los derechos ARCO como acceso, rectificación, cancelación y oposición.
	Juez 3		Aquí reitero el enfoque educativo y conciencia que se podría implementar en las escuelas como curso obligatorio así que también veríamos un mayor progreso en casa. Y por supuesto, una mayor supervisión y control por parte del Estado.
	Juez 4		A través de campañas de conciencia para informar a la población sobre los riesgos y beneficios de la era digital y la importancia de proteger sus datos personales.

Por otra parte, se entrevistó a los ingenieros del área de soporte informática del poder de judicial de Apurímac y Cusco

Donde:

Los ingenieros del soporte informático de Poder Judicial de Cusco son:

1. Ing. 1 (Cusco)
2. Ing. 2 (Cusco)

El ingeniero del soporte informático del Poder judicial de Apurímac es:

3. Ing. 3 (Apurímac)

Tabla 3: *Cuadro de transcripción de respuestas de entrevistados (Ingenieros).*

PREGUNTA A LOS INGENIEROS DEL SOPORTE INFORMÁTICO			**RESPUESTA**
Objetivo general: Analizar la protección legal del	**Ingeniero 1**	¿Cómo percibe el derecho a la autodeterminació n informativa en la gestión de datos	Se han tomado medidas a nivel de la gerencia de Lima, y seguridad de la información, controlando los equipos, usuarios (servidores judiciales).
	Ingeniero 2		Está relacionado con la ley de protección de datos personales, y acceso a la información.

derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano.		dentro del Poder Judicial?	Dentro del poder judicial sede cusco, para los servidores, es muy fácil acceder a información privado.
	Ingeniero 3		Son aquellas prácticas que ayudan a proteger la privacidad y los derechos de las personas, asegurando que el poder judicial maneje los datos de manera ética y legal.
	Ingeniero 1	¿Qué desafíos enfrenta el área de soporte informático para garantizar la protección de los datos personales en los sistemas digitales judiciales?	Los servidores judiciales prestan sus usuarios y contraseñas, para filtrar información. Los sistemas son seguros, quienes vulneran esa seguridad es el personal.
	Ingeniero 2		Los servidores comparten sus usuarios con otros servidores y eso facilita que se filtre información a terceros.
	Ingeniero 3		El área de soporte enfrenta varios desafíos importantes como la ciberseguridad, como las amenazas cibernéticas, como el malware, el phishing y los ataques de ransomware. También la gestión de accesos, como controlar quien tienen acceso a los datos personales, esta incluye implementar autenticación multifactor, gestionar permisos de usuarios y monitorear el acceso a los datos para prevenir accesos no autorizados.
	Ingeniero 1	¿Qué tan efectiva considera la implementación de políticas de seguridad y privacidad en los sistemas digitales judiciales?	Estamos a un 50%, recién nos estamos adaptando a los compromisos de ciberseguridad. La directiva se está cumpliendo a medias, en cuanto a la ciberseguridad, se necesita un oficial de seguridad en cada sede.
	Ingeniero 2		No, es tan efectiva, porque los estándares, son bajas y no están implementadas para proteger los datos judiciales.
	Ingeniero 3		En relativa, ya que aún estamos en un proceso de adaptación a las tecnologías. Sin embargo, estamos utilizando el uso de las tecnologías avanzadas como el cifrado de datos, la autenticación multifactor, ayudan a mejorar la seguridad digital judicial.
Objetivo específico 1: Describir de qué manera se protegen los datos personales generales frente a la era digital en el sistema constitucional peruano.	**Ingeniero 1**	¿Cómo percibe la regulación del derecho fundamental a la autodeterminación informativa en el sistema constitucional peruano?	Cada vez, los datos se están restringiendo más, a través de la autenticación de usuarios.
	Ingeniero 2		No, se está aplicando de forma efectiva e integra la ley de protección de datos personales.
	Ingeniero 3		Por este derecho se permite a las personas que puedan controlar su información personal que se recopila, almacena y utiliza sobre ellas. En el Perú está regulado en la Constitución y el Código Procesal Constitucional a través del Habeas Data.
	Ingeniero 1	¿Existen protocolos específicos en el Poder Judicial para garantizar la autodeterminación informativa de los ciudadanos en sus procesos judiciales?	Los protocolos son en relación al usuario, ya que solo los datos se proporcionan a quienes son parte del proceso y a sus abogados, no a terceros.
	Ingeniero 2		Existen protocolos, que envían a nivel central, sobre el acceso de usuarios y cambios de contraseñas. Esos protocolos cambian periódicamente, que son normativas que deben cumplir los usuarios.
	Ingeniero 3		Si, en el Poder Judicial existen protocolos específicos para garantizar la autodeterminación informativa de los ciudadanos en sus procesos judiciales como: protocolos de actuación, que ayudan a manejar los datos personales de manera adecuada, y las guías que nos envían desde la central del Poder Judicial.
	Ingeniero 1	¿Cómo se ha venido aplicando	De forma gradual, nos estamos ciñendo al plan de gobierno digital, solo hay un oficial de seguridad en

		la normativa sobre protección de datos personales en el Poder Judicial en los últimos años?	Lima, esta centralizado y se necesita un oficial de seguridad en todas las sedes.
	Ingeniero 2		No se está aplicando de forma íntegra los protocolos de seguridad y la ley de protección de datos personales.
	Ingeniero 3		Se ha venido aplicando de forma progresiva y con un enfoque de protección a los derechos fundamentales. El poder judicial aplica la ley 29733, que establece directrices claras sobre cómo se debe manejar los datos personales, asegurando su seguridad y confidencialidad.
Objetivo específico 2: Explicar de qué manera se encuentran protegidos los datos sensibles frente a la era digital en el sistema constitucion al peruano.	**Ingeniero 1**	¿Qué medidas ha implementado el Poder Judicial de Cusco y Apurímac para cumplir con la regulación sobre la era digital y la protección de datos?	En el año 2023, se están migrando las computadoras a un directorio activo, a fin de controlar y proteger los datos.
	Ingeniero 2		Se están aplicando los servidores informáticos como PROXY y FIREWALL, para proteger los datos.
	Ingeniero 3		El Poder Judicial de Apurímac ha implementado varias medidas para cumplir con la regulación de la era digital y la protección de datos personales desde la capacitación y concientización con el objetivo de sensibilizar y educar sobre la importancia de la protección de datos personales y las medidas de seguridad tecnológica.
	Ingeniero 1	¿Cómo se gestiona la seguridad informática para evitar filtraciones o accesos no autorizados a la información judicial?	A nivel de usuarios, desde el acceso a las computadoras, donde ciertos usuarios de acuerdo a su jerarquía tienen acceso a ciertos datos y expedientes.
	Ingeniero 2		A través del control del acceso de los usuarios, limitando sus accesos a cierta información, de acuerdo con su jerarquía de cargos. Ante ciber ataques, no recibimos alertas, pero en la sede central de Lima, se controla estos hechos.
	Ingeniero 3		Se utilizan los cifrados de datos para proteger la información sensible tanto en tránsito como en reposo. Esto asegura que los datos sean ilegibles para cualquier persona no autorizada que intente acceder a ellos. El control de accesos, donde se establecen políticas estrictas de control de acceso para garantizar que solo el personal autorizado pueda acceder a información judicial.
	Ingeniero 1	¿Qué tecnologías o herramientas se utilizan para garantizar el cumplimiento de la regulación digital en la administración de justicia?	Solo el directorio activo y el Firewall, a fin de prevenir, filtraciones y vulneraciones a nuestros datos. Sin embargo, se necesita proteger de forma descentralizada los datos de cada sede
	Ingeniero 2		Solo el control de seguridad de Windows y sus aplicaciones integradas. En cuanto al sistema integral judicial, se encuentra cifrado de extremo a extremo, solo en cuanto al acceso de usuarios.
	Ingeniero 3		El Rech Tech, diseñadas para facilitar el cumplimiento de las normativas legales y regulatorias. El Black chain, para asegurar la integridad y transparencia de los datos judiciales. El cifrado de datos para proteger la información sensible y garantizar que solo las personas autorizadas puedan acceder a ellas.
Objetivo específico 3: Determinar cómo se regula el consentimie	**Ingeniero 1**	¿Qué buenas prácticas o medidas de seguridad recomienda para fortalecer la	No acceder a correos, links sospechosos, los servidores judiciales deben proteger sus usuarios. Los magistrados y servidores deben cambiar sus contraseñas.
	Ingeniero 2		Los servidores judiciales tienen usuarios y contraseñas muy simples, de fácil predictibilidad por terceros.

nto informado frente a la era digital en el sistema constitucional peruano.		protección de los datos personales en los sistemas digitales judiciales?	Considero que deben cambiar contraseñas mensualmente, y no compartir los usuarios con otros servidores judiciales.
	Ingeniero 3		Actualización de sistemas y software actualizados es crucial para proteger los datos contra vulnerabilidades conocidas. Planes de respuestas a incidentes, para una reacción rápido y efectivo ante cualquier brecha de seguridad minimizando el impacto y recuperando la normalidad lo antes posible.
	Ingeniero 1	¿Existen iniciativas o proyectos en el Poder Judicial de Apurímac y Cusco para mejorar la seguridad y el control sobre la información digital de los ciudadanos?	No, porque todo lo relacionado a la ciberseguridad se controla desde la sede de Lima.
	Ingeniero 2		No, en la ciudad de Abancay, no ha presentado ninguna iniciativa.
	Ingeniero 3		Si, como la plataforma digital de transparencia que facilita el acceso a la información pública y mejora la transparencia en la administración de justicia que incluye servicios como la casilla electrónica y mesa de partes virtual. Y, capacitaciones en seguridad informática.
	Ingeniero 1	¿Qué medidas de ciberseguridad deberían fortalecerse para mejorar la protección de la autodeterminación informativa en el ámbito judicial?	Deberían comprar un buen Firewall, que sea manejado propiamente para la Ciudad de Abancay. En estos últimos años 2020 en adelante se ha filtrado fichas RENIEC, procesos cautelares y otros. Con un buen Firewall, se podría controlar de mejor manera la administración de los datos judiciales.
	Ingeniero 2		Básicamente, se deben aplicar los estándares de ciberseguridad. La corte de Cusco, debería invertir con un presupuesto, y capacidad del personal, para el correcto manejo de la información. Existe un uso irresponsable sobre el tratamiento de datos parte de los magistrados y servidores judiciales.
	Ingeniero 3		El cifrado de datos. Actualización de sistemas. Evaluaciones de riesgos de forma periódica. Se establecen políticas estrictas de control de accesos a bases de datos con los usuarios de jueces y servidores judiciales.

5.2. Resultado del análisis jurisprudencial.

5.2.1. Exp. N.º 3326-2019-0-1801-JR-DC-02: SIDPOL

Hechos: Sebastián Carlos Aguedo Zuñiga interpuso una demanda de hábeas data contra el Ministerio del Interior para eliminar su registro en el Sistema de Denuncias Policiales, luego del archivo de una investigación penal en su contra.

Primera y segunda instancia: El Segundo Juzgado Constitucional Transitorio de Lima declaro infundada la demanda. La Sala Superior confirmó el fallo de primera instancia,

señalando que el reglamento interno de la Policía Nacional del Perú no permite modificar la base de datos y el registro no genera antecedentes ni afectación actual.

Tribunal Constitucional: El TC (2021) estimó la demanda, estableciendo que la autodeterminación informativa comprende el derecho al olvido; donde la información que fue veraz, pero carece de sustento actual debe suprimirse si causa perjuicio. El máximo interprete ordenó a la parte demandada implementar medidas de resguardo de la privacidad.

Análisis: Se fija el criterio de caducidad del dato. La potestad policial de almacenar información es legítima, pero está condicionada a los principios de veracidad, finalidad y temporalidad.

5.2.2. Exp. N.º 786-2020-0-2001-JR-CI-02: Facebook no constituye banco de datos

Hechos: Edward Antonio Muñoz Salazar planteó hábeas data inquisitivo contra José Alfredo Infante Carmen para identificar al responsable de divulgar sus datos personales en Facebook.

Primera y segunda instancia: El Segundo Juzgado de Piura declaró infundada la demanda. La Sala Civil ratificó la misma, señalando que el hábeas data inquisitivo tutela el acceso a registros existentes, no la revelación de fuentes.

Tribunal Constitucional: El TC declaró improcedente la demanda. Precisó que una cuenta personal de Facebook no califica como "banco de datos" según la Ley N.º 29733, por lo que el hábeas data no es vía idónea para reclamar difusión de información en redes sociales.

Análisis: Se delimita el objeto del hábeas data señalando que solo procede contra registros organizados, públicos o privados, no contra publicaciones en plataformas digitales.

5.2.3. Exp. N° 696-2021-0-2301-SR-CT-03: Titularidad del número telefónico

Hechos: Francisco Rómulo Apaza Suca demandó a Telefónica del Perú S.A.A. para conocer al titular de líneas telefónicas que lo hostigaban mediante SPAM.

Primera y segunda instancia: El Tercer Juzgado Civil de Tacna declaró improcedente la demanda. La Sala confirmó la misma, señalando que la titularidad está amparada por el secreto de las comunicaciones.

Tribunal Constitucional: El TC (2022) declaró fundada la demanda, y determinó que el número telefónico es dato personal y su tratamiento exige consentimiento. Sin embargo, la parte demandada, vulneró la autodeterminación informativa al no acreditar titularidad ni negar el dato, impidiendo ejercer el derecho a oposición.

Análisis: Se consolida el criterio de que el número celular es un dato personal. Las operadoras deben acreditar consentimiento o brindar información ante acoso.

5.2.4. Exp. N° 2553-2021-0-1001-JR-CI-03: Difusión de imágenes íntimas

Hechos: Se demandó vía hábeas data el cese de difusión no consentida de fotos y videos íntimos de una señorita en un grupo de WhatsApp.

Fallo: El Juzgado Civil de Santiago-Cusco declaro fundada la demanda, y ordenó suprimir los datos íntimos en todo soporte digital.

Análisis: La sentencia se extendió el derecho a la autodeterminación informativa a registros privados electrónicos, donde la tutela no se restringe a bases organizadas privadas con alcance social como grupos de WhatsApp.

5.2.5. Exp. N° 73-2022-0-0301-JR-C1-02: Derrama Magisterial

Hechos: Ramiro Rojas Cortez demandó a la Derrama Magisterial el acceso a informes financieros de sus aportes, invocando la Ley N° 27806.

Primera y segunda instancia: El Segundo Juzgado Civil de Abancay declaró infundada la demanda. La Sala confirmó que la misma, aduciendo que la Derrama es una persona jurídica privada que no presta servicios públicos, por lo que no aplica la ley de transparencia.

Tribunal Constitucional: El TC (2023) declaró fundada en parte la demanda. Diferenció que, la Derrama no presta servicio público, no obstante, el asociado tiene derecho a acceder

a sus datos personales (autorización de descuento y estado de cuenta), por ser titular de los mismos.

Análisis: Se distingue acceso a información pública vs. autodeterminación informativa. El asociado puede exigir sus propios datos.

5.2.6. Exp. 900-2021-0-JR-CI-04: Notificación a Mark Zuckerberg

Hechos: Juan Mejía Seminario demandó a Mark Zuckerberg por la suspensión de su cuenta de Facebook en tiempos de pandemia. El Cuarto Juzgado Civil de Piura dispuso un exhorto diplomático por intermedio del Ministerio de Relaciones Exteriores.

Aspecto relevante: Entre los años 2021-2025 el proceso permanece paralizado por ausencia de un traductor. El hábeas data, siendo un proceso sumarísimo por naturaleza, se desnaturalizo por formalismos de notificación a plataformas transnacionales.

Análisis: Se evidencia indefensión procesal en la era digital. El derecho del demandante queda postergado al no poder emplazar a plataformas globales, volviendo la sentencia en un acto procesal meramente declarativa.

***Tabla 4**: Cuadro de análisis de sentencias de habeas data emitidas por el Tribunal Constitucional que establecen aspectos fundamentales relacionados con la era digital.*

Exp N°01116-2022-PHD/TC	**FJ.13** Un dato personal, cuyo consentimiento es necesario para su tratamiento, es el número telefónico, esto porque el acceso a dicho dato permite, a quien inicie su tratamiento, tener acceso directo a su titular ya sea a través de llamadas telefónicas o a través del uso de aplicaciones de mensajería, situación que de haberse efectuado son consentimiento, decaería en una conducta infractora grave; sin embargo, tal conducta se transforma en doblemente lesiva cuando quien viene haciendo dicho tratamiento obstaculiza los medios que razonablemente permitirían el ejercicio del derecho de oposición al tratamiento de datos personales.
Exp N°01163-2022-PHD/TC	**FJ.17** En consecuencia, si bien de acuerdo a la LPDP pueden considerarse como datos personales los "destinados a ser contenidos en bancos de datos"24, como sería Facebook, la ley no es aplicable a las cuentas personales de los usuarios por expresa exclusión que hace de ellas la norma mencionada, en su primer apartado, cuando establece que no afecta "a los contenidos o destinados a ser contenidos en bancos de datos personales creados

	por personas naturales para fines exclusivamente relacionados con su vida privada o familiar”
Exp N°02839-2021-PHD/TC	**FJ.13** En el presente caso, nos encontramos sin embargo con determinadas particularidades sobre las que conviene tomar atención, pues aunque el Ministerio del Interior alega que el registro que efectivamente posee la Dirección de Criminalística de la Policía Nacional del Perú, no tiene carácter público ni debería ser de acceso a terceros, no ha podido evitar en los hechos que el mismo pueda ser utilizado por empresas como VOCATI CONSULTING, siendo totalmente irrelevante que califique dicho acceso como simplemente ilegal sin que a su turno haya podido tomar las previsiones del caso.

5.3. Resultado de análisis normativo.

Se realizó también un análisis de las principales normas relevantes, relacionándolas con las categorías de mi investigación, que a continuación detallo:

5.3.1. Ley N° 29733 – Ley de Protección de Datos Personales

Finalidad: Regular el tratamiento de datos personales en el ámbito público y privado, garantizando que se realice con consentimiento del titular y en respeto estricto de los derechos fundamentales de todo ciudadano (Ley N° 29733, 2011).

Análisis: Constituye el principal instrumento normativo que desarrolla el derecho fundamental a la autodeterminación informativa reconocido en el art. 2, inc. 6 de la Constitución, pero de forma implícita.

Resumen: Materializa este derecho mediante los derechos ARCO permitiendo al titular administrar integralmente sus datos.

5.3.2. Decreto Supremo N° 016-2024-JUS (Reglamento de la Ley N° 29733)

Finalidad: Actualizar el sistema de protección de datos personales frente a los riesgos tecnológicos actuales (Decreto Supremo N° 016-2024-JUS, 2024).

Análisis: Fortalece la autodeterminación informativa al incorporar mecanismos de protección digital, como un mecanismo preventivo ante tratamientos de alto riesgo; decisiones automatizadas; obligación de reportar filtraciones; e incorpora la figura obligatoria de oficiales de datos.

Resumen: Evidencia la evolución del constitucionalismo digital peruano, extendiendo su protección al entorno digital complejo.

5.3.3. Decreto Legislativo N° 1412 – Ley de Gobierno Digital

Finalidad: Promover la transformación digital del Estado mediante servicios públicos digitales interoperables (Decreto Legislativo N° 1412, 2018).

Análisis: El gobierno digital está orientado al tratamiento masivo de datos personales por parte del Estado. Por ello, la autodeterminación informativa opera como límite constitucional al poder tecnológico estatal en la prestación de servicios.

Resumen: Autoriza el intercambio de información entre entidades, fortalece la identidad y ciudadanía digital.

5.3.4. Decreto Supremo N° 029-2021-PCM – Reglamento de la Ley de Gobierno Digital

Finalidad: Regular las condiciones, requisitos y procedimientos para la implementación del gobierno digital (Decreto Supremo N° 029-2021-PCM, 2021).

Análisis: Busca equilibrar la eficiencia estatal y la protección de derechos fundamentales. Sin embargo, existe un riesgo debido a la centralización de información sensible.

Resumen: Define los alcances institucionales en gestión de datos y confianza digital, exigiendo que los servicios digitales estén enfocados en el ciudadano.

5.3.5. Decreto de Urgencia N° 006-2020 – Sistema Nacional de Transformación Digital

Finalidad: Crear el Sistema Nacional de Transformación Digital e impulsa la digitalización en la prestación de servicios (Decreto de Urgencia N° 006-2020, 2020).

Análisis: La digitalización estatal incrementa el flujo de datos personales, por lo que requiere garantías reforzadas de privacidad y seguridad digital.

Resumen: Fomenta el uso de plataformas y servicios electrónicos, imponiendo deberes de seguridad y confianza digital a las entidades.

5.3.6. Ley N° 31814 – Ley que promueve el uso de la Inteligencia Artificial

Finalidad: Fomenta el desarrollo y uso responsable de la inteligencia artificial (Ley N° 31814, 2023).

Análisis: La IA plantea desafíos relevantes para la protección de datos. Riesgos como el perfilamiento digital, el cual permite construir perfiles de información sin consentimiento del titular, afectando la autodeterminación informativa.

Resumen: Promociona el uso de esta herramienta tecnológica en aspectos educativos y económicos.

5.3.7. Decreto de Urgencia N° 007-2020 – Marco de Confianza Digital

Finalidad: Garantizar la seguridad en entornos digitales. (Decreto de Urgencia N° 007-2020, 2020).

Análisis: La confianza digital es una condición para el ejercicio seguro de derechos en entornos virtuales. Reconoce implícitamente que la protección de datos personales integra el núcleo esencial de los derechos fundamentales en la era digital.

Resumen: Fortalece la protección de la identidad digital y desarrolla acciones estatales en materia de ciberseguridad.

5.3.8. Decreto Supremo N° 085-2023-PCM – Política Nacional de Transformación Digital al 2030

Finalidad: Se encuentra orientado al proceso de transformación digital del país hasta el año 2030 (Decreto Supremo N° 085-2023-PCM, 2023).

Análisis: Reconoce la necesidad de un entorno digital centrado en la persona y la prestación de servicios estatales. Su éxito depende de la capacidad institucional, y educación digital.

Resumen: Promueve la innovación tecnológica, y servicios públicos digitales como ejes transversales.

5.4. Discusión de resultados

De acuerdo con las entrevistas, se puede examinar en profundidad la información de cada participante siguiendo el procedimiento del Habeas Data, tomando en cuenta la jurisprudencia revisada, la Ley de Protección de Datos Personales y su Reglamento, siempre en línea con los objetivos planteados:

5.4.1. Objetivo General

Analizar la protección legal del derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano.

En cuanto al objetivo general, se realizó a los magistrados entrevistados la pregunta **¿Cómo analizan e interpretan el derecho fundamental a la autodeterminación informativa en el sistema constitucional peruano?**; estos coinciden en que el derecho a la autodeterminación informativa es un pilar esencial que otorga a los individuos la libertad y la conciencia de administrar el manejo de sus datos personales de manera libre y consciente. El Juez 1 lo conecta de manera directa con el derecho a la salvaguarda de datos personales, subrayando la potestad de decidir por cuenta propia sobre los datos recopilados, guardados

y administrados por terceros. El Juez 2 subraya la importancia de salvaguardar la confidencialidad, la imagen, la identidad individual y familiar ante el manejo de información digital. Para el magistrado 4, la autodeterminación informativa no solo es un derecho de supervisión, sino que se encuentra en peligro por fenómenos como la vigilancia masiva, la minería de datos y la circulación de información sin consentimiento. Finalmente, el juez 3**,** presidente de la Sala Civil, plantea que este derecho ya está reconocido en la Constitución, pero admite que la era digital ha aumentado su exposición y vulnerabilidad de la información personal.

Estos aportes reflejan una comprensión garantista del derecho, cercana a lo desarrollado por Linares (2019)**,** quien sostiene que la autodeterminación informativa posee autonomía conceptual frente a otros derechos conexos como la intimidad o el secreto de las comunicaciones, y requiere protección específica.

Asimismo, la visión judicial recogida en las entrevistas se alinea con lo propuesto por Landa (2017)**,** quien señala que el control de los datos implica no solo el acceso a ellos, sino también su modificación, cancelación o supresión, lo cual exige consentimiento informado frente a cualquier tratamiento.

Desde la perspectiva constitucional y jurisprudencial, el derecho a la autodeterminación informativa puede concebirse como una prerrogativa implícita en el artículo 2, numeral 6 de la Constitución Política del Perú, reforzada por el artículo 3, que reconoce otros derechos no expresamente mencionados. El Tribunal Constitucional, en el expediente N°05854-2005-PA/TC, establece que los derechos fundamentales deben interpretarse conforme al principio *pro homine*, buscando siempre el mayor nivel de protección para la persona. También reconoce el principio del *control de convencionalidad*,

lo que obliga al Estado peruano a garantizar este derecho conforme a los tratados internacionales que ha ratificado.

Ese enfoque se complementa con el aporte de Viveros (2018)**,** quien en su tesis sobre la autodeterminación informativa en Chile evidencia cómo la tecnología puede desbordar los marcos normativos tradicionales, generando vacíos legales que permiten la vulneración de datos sensibles como los genéticos. Esa realidad investigada refleja una situación parecida en el Perú, donde la legislación en cuanto a protección de datos, sobre todo "Genéticos", presenta un vacío legal, frente al avance tecnologías innovadoras y la creciente adopción de medios digitales.

Asimismo, el entorno de la cuarta revolución industrial descrito por Villar (2019) aporta el marco socio tecnológico donde este derecho debe ejercerse: un entorno globalizado, interconectado y digitalizado que exige nuevos enfoques legales, éticos y organizacionales.

En este contexto, se puede afirmar que el derecho fundamental a la autodeterminación informativa consiste en la facultad de cada persona para gestionar su información, compuesta por datos de diversa índole, que están bajo custodia de bases de datos públicos o privados; siendo un derecho autónomo pero si relacionado a otros derechos como la imagen, la dignidad, privacidad y otros, y que actualmente se enfrenta a desafíos como la vigilancia masiva, la minería de datos y la circulación de información sin consentimiento.

Así también, se les realizo la consulta sobre, **¿Cuáles han sido los principales desafíos que ha enfrentado el sistema judicial en la protección del derecho fundamental a la autodeterminación informativa frente al avance de la era digital?**; el juez 1 y el magistrado 4, coinciden en que la era digital viene avanzando de manera acelerada, hecho

que incluso ha superado la capacidad del sistema judicial para proteger adecuadamente el derecho fundamental a la autodeterminación informativa. El magistrado 4 también señala que los magistrados no se encuentran capacitados para abordar temas relacionados con la protección de datos frente a la era digital; y según el magistrado 3, no hay una normativa precisa y vigente sobre datos personales; además, en la práctica, este derecho debe ser equilibrado con otros como la libertad de expresión y el acceso a la información.

Lo señalado por el magistrado 3 refleja la realidad jurídica actual, dado que la Constitución de 1993 protege y reconoce de forma tácita este derecho en su artículo 2, numeral 6; además, se asegura mediante la garantía constitucional del Habeas Data establecida en el artículo 200, numeral 3, la Ley de Protección de Datos Personales de 2011 y su reglamento emitido en noviembre de 2024, como respuesta a los nuevos desafíos de la era digital; asimismo, está contemplado en el Nuevo Código Procesal Constitucional publicado en 2021; como puede advertirse solo contamos con dos normativas publicadas en esta década.

Sin embargo, para el magistrado 3 esto no resulta suficiente, ya que nos encontramos ante una regulación que no es clara, y sobre todo en su aplicación e interpretación llega a enfrentarse con otros derechos, como el de la libertad de expresión. Este hecho incluso fue evidenciado con lo resuelto en el Exp N°01163-2022-PH/TC, donde un accionante solicitaba a un usuario de Facebook que brinde información sobre la fuente sobre quien le suministro su información personal, para el Tribunal Constitucional, el proceso del Habeas data no es el mecanismo adecuado para atender la solicitud del usuario, ya que, desde su punto de vista, una cuenta de Facebook no se considera un banco de datos. En el fundamento 17 de la misma sentencia, se indica que “La Ley de Protección de Datos Personales no se aplica a las cuentas personales, porque no corresponde a los contenidos o datos almacenados en bancos de datos

personales creados por personas naturales para fines exclusivamente vinculados a su vida privada y familiar".

Desde mi punto de vista, no coincido con la decisión del Tribunal, pues consideró que una cuenta de Facebook sí constituye un banco de datos, ya que, a través de ella se puede difundir información diversa que, dada su rapidez en el entorno digital, puede alcanzar inmediatamente a muchas personas. En este escenario, por un lado, está quien ejerce su derecho a la libre expresión y, por otro, el demandante cuya dignidad resulta afectada por las publicaciones obtenidas. Mediante un test de ponderación, la pretensión del demandante debío haber sido declarada fundada, ya que se vulneró su derecho a la autodeterminación informativa y su dignidad en las redes sociales del demandante.

La decisión del Tribunal Constitucional evidencia que, en realidad, los magistrados no cuentan con el conocimiento suficiente sobre los avances de la era digital, ni sobre cómo se vulneran los datos personales en ese ámbito, ya que conforme incluso la Ley de Protección de Datos personales, Articulo 2 numeral 1 "es un conjunto organizado de datos personales", y una cuenta personal de Facebook si viene a tener la naturaleza de un banco de datos, ya que permite recopilar, analizar, eliminar, acceder y transferir información; y en la praxis existen muchos usuarios que se dedican a utilizar sus cuentas personales para transmitir información ya sean desde noticias entre otros, lo que demuestra que usuarios de Facebook vienen utilizando sus redes sociales excediéndose de la utilidad por la cual fue creada, que es socializar con amigos y familiares, ya que, lo que está ocurriendo en la realidad estas cuentas están siendo utilizadas gestionando datos de diferente naturaleza sean sensibles o no, con la finalidad de generar hechos noticiosos, que pueden llegar a afectar la dignidad de las personas de las cuales se realizan estas publicaciones, inclusive compartiendo información que no cumplen con los filtros de veracidad, de los cuales los

propietarios de dichas de plataformas deberían estar en constante verificación y fiscalización, hecho que no ocurre.

Así también, se realizó la siguiente pregunta a los magistrados entrevistados **¿Consideran que la normativa vigente es suficiente para garantizar el derecho fundamental a la autodeterminación informativa en la era digital o requieren reformas?**; todos los magistrados coincidieron que la normativa actual, no es suficiente para abordar los desafíos que trae la era digital, el Juez 1 señaló que en la actualidad el proceso del habeas data, termina siendo un proceso largo lo cual se desnaturaliza ya que debería ser sumario y urgente, y más aún cuando se tienen como pretensiones la supresión o el ejercicio del derecho al olvido en el mundo virtual, ya que mientras el proceso se encuentre en trámite, los datos se encuentran allí y se difunden a gran velocidad, lo cual puede agravar la situación del justiciable, hecho que en la realidad si ocurre tal como lo resuelto el expediente N°02839-2021-PHD/TC, donde se encontraban datos de un accionante en el sistema SIDPOL-PNP, y que a pesar de que el registro de una denuncia se encontraba archivada, le perjudicaba en cuanto al encontrar un trabajo y su dignidad, ya que ese dato consignado en dicho registro ya tenía la calidad de "inexacto", el problema suscitado fue que terceros como una empresa privada denominada VOCATI CONSULTING, tenía acceso a estos datos que, cabe recalcar se encontraban administradas bajo una entidad pública que es la Policía Nacional del Perú, mientras el proceso se encontraba en trámite conforme a los antecedentes expuestos en esta jurisprudencia se interpuso un 7 de junio del 2019, y termino siento resuelto un 22 de agosto del 2022, es decir casi tres años, lo cual obviamente no resulta prudente, ni mucho menos cumple con la finalidad del proceso del habeas data que tiene que ser un proceso célere y urgente.

En esa misma línea, el Juez 1, evidencio que el proceso del Habeas data termina siendo un proceso mucho más largo ya sea desde el emplazamiento hasta la ejecución de sentencias, y se da en el contexto cuando se trata de un banco de datos que se encuentra bajo la administración de empresas internacionales, que tienen como domicilio el extranjero, y que incluso en el caso de ejecución de sentencias, no se podrían ejecutar alegando la falta de jurisdicción.

El procedimiento específico del Habeas Data está regulado en el artículo 53 del Nuevo Código Procesal Constitucional, que establece como requisito previo haber presentado la solicitud correspondiente al demandado para la protección del derecho a la autodeterminación informativa, y en caso de ser atendido de forma incompleta o de no serlo en el plazo de 10 días, puede acudir a la vía jurisdiccional, dentro de los 60 días de sufrida la afectación a su derecho.

Una vez iniciado el proceso jurisdiccional, que es con el auto admisorio de la demanda, el juez señala fecha y hora para realizarse la audiencia única dentro de los treinta días de admitida la demanda, así también le otorga 10 días hábiles al demandado para que conteste la demanda, y el juez tiene 10 días después de realizar la audiencia única para emitir sentencia, todo esto conforme al artículo 12 del Nuevo Código Procesal Constitucional; de lo que se puede concluir que un proceso de habeas data, en primera instancia debería durar un aproximado de 40 días hábiles, hecho que en la praxis y por el principio de realidad no ocurre, tal como lo manifestado por el Juez 1, quien señala que este proceso termina siendo mucho más largo, según las particularidades de cada situación, y especialmente cuando el demandado sea una entidad internacional, que tenga como domicilio su país de origen, hecho que genera un retraso con el curso del proceso, porque la debida notificación que es el emplazamiento debe garantizarse a fin de cumplir el debido proceso.

En ese mismo sentido, todos los magistrados entrevistados, coinciden que la normativa procesal vigente, no resulta suficiente para abordar los desafíos que trae la era digital, y que incluso requieren reformas, los jueces 1 y 2 hicieron hincapié en señalar que, la normativa no regula aspectos como la Inteligencia Artificial, ya que a través de ellas se puede transformar imágenes, suplantar identidad, voz y otros.

Esta situación es real, ya que el legislador publicó el Decreto Supremo N°016-2014-JUS (Reglamento de la Ley de Protección de Datos Personales) el 30 de noviembre de 2024, con menos de un año de vigencia. Sin embargo, ni dicho reglamento, ni la Ley de Protección de Datos Personales establecen de manera explícita los límites o condiciones para el uso de la Inteligencia Artificial, pese a ser ambos instrumentos legales aplicables en los procesos de hábeas data. En ese sentido resulta importante que ambos instrumentos legales, deberían abordar estas problemáticas ya que la Inteligencia Artificial requiere acceder a un gran volumen de banco de datos a fin de brindar información a lo solicitado por el usuario, a fin de tomar decisiones automatizadas sin intervención humana, afectando de esa forma el derecho a la autodeterminación informativa, tal como lo ocurrido en las elecciones presidenciales de Estados Unidos ocurrido en el año 2016.

En ese sentido, la Ley N° 31814, conocida como “Ley que impulsa el uso de la inteligencia artificial para el desarrollo económico y social del país”, establece en su artículo 3, literal “B”, que la inteligencia artificial está creada para realizar predicciones, recomendaciones o tomar decisiones. Sin embargo, esta norma no enfatiza que el uso de la inteligencia artificial tiene como limites el respeto de los derechos fundamentales como la autodeterminación informativa y la dignidad, entre otros.

Como resultado, ante las inquietudes expresadas por los magistrados entrevistados sobre la insuficiente regulación procesal del derecho a la autodeterminación informativa

frente a la era digital, así como la Ley de Protección de Datos Personales y su reciente reglamento, se concluye que estas, son insuficientes frente a los avances tecnológicos actuales. Además, el proceso de Habeas Data debería contemplar la implementación de una notificación electrónica validada para notificar a empresas internacionales que gestionan bancos de datos. Asimismo, la ejecución de las sentencias demanda un alto nivel de cooperación internacional, siempre respetando el debido proceso.

Por otro lado, desde un enfoque técnico, en la presente investigación resulto necesario entrevistar a los ingenieros del área de soporte informático del Poder Judicial, ello en razón de la naturaleza donde desempeñan sus funciones, y sobre todo porque el Poder Judicial, viene a ser una entidad que maneja una gran base de datos de los justiciables, datos de distinta índole y sensibilidad; los ingenieros en cuanto al objetivo general que es analizar la protección legal del derecho fundamental a la autodeterminación informativa, conforme a su percepción de este derecho dentro de la gestión de datos dentro del Poder Judicial, reconocen a este derecho y lo relacionan con la Ley de protección de datos personales y el acceso a la información, así también el ingeniero 3 vincula este derecho directamente con aquellas prácticas que ayudan a proteger la privacidad y derechos de las personas; mientras que el ingeniero 1 lo relaciona con los esfuerzos institucionales por proteger los datos personales en el entorno judicial, mediante medidas como la autenticación multifactor, el cifrado de datos y la gestión de accesos.

Así también, los tres ingenieros destacan las significativas deficiencias del área de soporte informático para asegurar la protección de datos personales, lo que revela importantes vulnerabilidades de este derecho en la era digital, por ejemplo, denuncian prácticas inseguras como el préstamo de credenciales entre servidores judiciales, el

incumplimiento de políticas básicas de seguridad, y una limitada cultura institucional de protección de datos.

En cuanto a la efectividad de la implementación de políticas de seguridad y privacidad de los sistemas digitales judiciales; a juicio de estos profesionales, los sistemas informáticos del Poder Judicial son relativamente seguros desde el punto de vista técnico, pero su efectividad se ve socavada por acciones humanas que vulneran los protocolos establecidos.

Esta situación coincide con su percepción de que la implementación de políticas de seguridad está solo a un 50% de efectividad, debido a la falta de oficiales de seguridad informática en cada sede y al bajo nivel de cumplimiento de las directivas internas. Además, destacan que el proceso de adaptación a las nuevas exigencias digitales aún está en marcha, lo que impide una protección integral y efectiva de los datos judiciales.

A pesar de ello, valoran positivamente los avances logrados, y apuestan por fortalecer la formación del personal y la institucionalización de estándares más rigurosos de ciberseguridad.

Bajo todo lo expuesto, en cuanto al objetivo general desde una óptica jurisdiccional, técnica, doctrinaria y jurisprudencial, por este derecho se establece que, el derecho fundamental a la autodeterminación informativa es un derecho independiente a otros derechos como la imagen, intimidad, privacidad y entre otros, ya que por el ejercicio de este derecho se puede garantizar el respeto irrestricto de otros derechos, y que en un estado actual de cosas frente a los avances de la era digital no se encuentra protegido adecuadamente en el sistema constitucional peruano.

El derecho fundamental a la autodeterminación informativa también puede entenderse como un derecho de acción protegido por la garantía constitucional del habeas data. Esta garantía asegura que toda persona tenga el control sobre la información que está registrada en bases de datos tanto públicas como privadas. Dentro del ejercicio de este control, el ciudadano tiene la facultad de conocer qué datos se almacenan, cómo se utilizan, quién los ha recopilado, realizar actualizaciones y solicitar la eliminación de aquellos datos que afecten o vulneren otros derechos. Así también, por este derecho se garantiza que todo uso de datos debe ser con expreso conocimiento y autorización de su titular.

En cuanto a una perspectiva procesal dentro del sistema constitucional, el proceso del habeas data, el legislador debería adecuar esta vía procesal a situaciones como el emplazamiento y ejecución de resoluciones, cuando el demandado se trate de una entidad internacional, con domicilio internacional, así también se deberían fortalecer la cooperación internacional a fin de salvaguardar el derecho fundamental a la autodeterminación informativa, frente a los nuevos desafíos que trae la era digital.

5.4.2. Objetivos Específicos

5.4.2.1. Objetivo específico 1

Describir de qué manera se protegen los datos personales generales frente a la era digital en el sistema constitucional peruano.

A fin de identificar la protección legal de datos generales, se realizó a los magistrados la siguiente consulta ¿Cómo está regulado el derecho fundamental a la autodeterminación informativa en el sistema constitucional peruano?, de sus respuestas se permitió analizar que tanto los jueces con competencia constitucional, como los ingenieros del área de soporte informático del Poder Judicial de Apurímac y Cusco, identifican una base normativa clara

constitucional a la autodeterminación informativa, aunque reconocen que su implementación actualmente enfrenta vacíos, disputas y restricciones ante los retos tecnológicos modernos.

Los magistrados entrevistados coinciden en señalar que este derecho está fundamentado principalmente en el artículo 2, inciso 6, de la Constitución Política del Perú, la Ley N° 29733 sobre Protección de Datos Personales, su reglamento correspondiente, así como en el Título IV del Código Procesal Constitucional, a partir del artículo 53°, destacando en particular el procedimiento constitucional del hábeas data.

De esta manera, el Juez 1 destaca que este entramado legal brinda a las personas la facultad de manejar sus datos personales y ejercer sus derechos ante el Estado o empresas privadas. En sintonía con esta perspectiva, el juez 2 subraya que el hábeas data ofrece la posibilidad de acceder, rectificar, suprimir o actualizar datos personales, estableciendo así una ruta judicial para ejercer el derecho a la autodeterminación informativa.

De manera más holística y armoniosa, el magistrado 4 amplía la mirada indicando que la regulación no solo se basa en normas escritas, sino también en la jurisprudencia y la doctrina, que aportan criterios interpretativos y principios que fortalecen la protección de este derecho en el entorno digital. A su vez, el magistrado 3 reafirma esta postura, pero también reconoce que, aunque la ley existe, no aborda con suficiente precisión los problemas actuales de la era digital.

Bajo esas premisas podemos establecer lo siguiente, el derecho fundamental a la autodeterminación informativa se encuentra:

1. En la Constitución artículo 2, numeral 6, en ejercicio de la garantía constitucional contemplada en el artículo 200 del mismo cuerpo legal, que el habeas data procede ante vulneraciones al acceso a información y autodeterminación informativa (Republica, 1993)

Se puede observar que la legislación constitucional no establece de manera expresa el derecho fundamental a la autodeterminación informativa; sin embargo, este derecho se infiere de dicha norma, dado que su objetivo es resguardar la información que puede afectar derechos como la privacidad personal y familiar. Por lo tanto, se trata de una protección tácita orientada a garantizar que todas las personas puedan ejercer control sobre su información personal.

En ese contexto, el derecho fundamental a la autodeterminación informativa concede al titular de los datos personales la facultad de resguardar su información ante posibles riesgos ocasionados por un uso inapropiado, conforme a lo establecido en el artículo 2, numeral 6, de la Constitución.

2. A través de la Garantía Constitucional del Habeas Data reconocido en el artículo 200 numeral 3 de la Constitución donde señala: “La acción de habeas data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2 incisos 5 y 6 de la Constitución.” (Constitución Política del Peru, 1993)

Esta garantía constitucional tiene como propósito permitir que las personas conozcan qué información posee una entidad, ya sea pública o privada, sobre ellas. En caso de que estos datos sean erróneos, estén desactualizados o resulten perjudiciales, pueden solicitar su corrección, actualización, eliminación o que se mantengan bajo reserva. De este modo, se busca proteger la privacidad, la intimidad y la dignidad frente a un uso inadecuado de la información personal. Aunque la Constitución no emplee expresamente el término “autodeterminación informativa”, el fundamento de este derecho radica en asegurar que cada uno tenga el control para elegir sobre sus datos.

3. Procesalmente se garantiza este derecho a través del Nuevo Código Procesal Constitucional Articulo 53; donde el proceso del habeas data, tiene como finalidad proteger dos derechos como el derecho fundamental al acceso a la información pública y proteger el derecho fundamental a la autodeterminación informativa.

Según la exposición de motivos de esta garantía constitucional, el proceso se define como un mecanismo especializado para que las personas puedan ejercer control sobre sus datos, incluyendo el derecho a conocer, actualizar, rectificar o suprimir la información que gestionan entidades públicas o privadas. Este procedimiento fue diseñado para ser rápido y sumario, dada la posible gravedad de los daños irreparables que puede ocasionar el mal uso de los datos personales al derecho fundamental a la autodeterminación informativa.

Aunque la normativa procesal no desarrolla expresamente el contenido del derecho a la autodeterminación informativa, su protección se infiere del artículo 2, numeral 6 de la Constitución Política del Perú (1993), la Ley N° 29733 (2011) y la jurisprudencia del Tribunal Constitucional.

El Tribunal Constitucional ha precisado los alcances de este derecho en su fundamento jurídico 8 del Expediente N° 01163-2022-PHD/TC, señalando que:

La protección del derecho a la autodeterminación informativa a través del hábeas data comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información, así como las personas que recabaron dicha información. En segundo lugar, el hábeas data puede tener la finalidad de agregar datos al

registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados. (Tribunal Constitucional del Perú, 2022, p. 4)

4. La Ley N° 29733 (2011) protege los datos personales y obliga a empresas y entidades públicas a pedir permiso antes de usarlos. El consentimiento debe ser previo, informado y expreso (Ley N° 29733, 2011, art. 13), y deben explicar para qué se usarán los datos y permitir que el titular los vea, corrija, suprima o incluso se oponga a su uso (Ley N° 29733, 2011, arts. 19-20). Si incumplen, reciben multas de 0.5 a 100 UIT (Ley N° 29733, 2011, art. 39). Aunque, la ley no menciona textualmente la “autodeterminación informativa”, este derecho se protege porque el art. 10 establece que el titular debe tener vías legales para defender sus datos (Ley N° 29733, 2011, art. 10).

5. El Reglamento de la Ley N° 29733, aprobado por Decreto Supremo N° 016-2024-JUS, desarrolla la Ley de Protección de Datos Personales para su aplicación efectiva (Decreto Supremo N° 016-2024-JUS, 2024).

Su finalidad es que las entidades públicas y privadas traten los datos personales respetando la intimidad, y privacidad de las personas. Ante presuntos incumplimientos, el reglamento prevé medidas correctivas (Decreto Supremo N° 016-2024-JUS, 2024, art. 122) y multas coercitivas (Decreto Supremo N° 016-2024-JUS, 2024, art. 130).

De lo expuesto, el derecho fundamental a la autodeterminación informativa no está expresamente regulado en la Constitución Política de 1993, pero se encuentra implícitamente en el artículo 2, numeral 6, así como en la garantía constitucional del hábeas data contenida en el artículo 200, numeral 3. Además, se encuentra respaldado por el Nuevo Código Procesal Constitucional a través del proceso del hábeas data regulado en el artículo 53, por la Ley N° 29733 de Protección de Datos Personales y su reglamento. Asimismo, la máxima autoridad constitucional ha señalado, mediante su jurisprudencia emitida, que el proceso del hábeas data es el mecanismo constitucional por excelencia para proteger este derecho fundamental.

Así también, se consultó a los magistrados ¿Qué aspectos normativos han sido objeto de mayor debate o controversia en cuanto a la regulación legal del derecho a la autodeterminación informativa?; todos los jueces destacan el derecho al olvido como una figura en discusión, especialmente frente a su aplicación práctica en medios digitales, motores de búsqueda y redes sociales.

Este tema también fue abordado en el Expediente N° 02839-2021-PHD/TC, donde en su fundamento 9 el tribunal destacó que el avance tecnológico ha provocado una gran acumulación de datos de diversas clases, lo que puede afectar la esfera protegida del derecho a la protección de datos. Asimismo, en su fundamento 10 se indicó que los datos inexactos pueden causar daños a otros derechos, por lo que el derecho al olvido busca prevenir que con el tiempo dicha información errónea perjudique otros derechos.

El juez 2 destacó que un tema frecuente es el consentimiento informado; en un entorno marcado por tecnologías como el big data, surge la duda sobre si las personas comprenden verdaderamente el alcance del tratamiento de sus datos personales. Esta situación refleja una preocupación auténtica respecto al equilibrio entre el derecho a la

información y la privacidad, aspecto que también señala el magistrado 4, quien enfatiza la necesidad urgente de actualizar el sistema normativo.

En esa misma línea se realizó la siguiente consulta a los magistrados, ¿Existen vacíos normativos o conflictos legales en la regulación de este derecho? Los jueces coincidieron en señalar deficiencias importantes.

Entre ellas; la falta de regulación específica para las nuevas tecnologías; la determinación sobre si las personas jurídicas pueden ser titulares de datos personales; la escasa claridad en el uso de datos en redes sociales; la debilidad frente a fenómenos como la vigilancia digital y la acumulación indiscriminada de información.

En ese sentido, los jueces proponen como necesidad urgente la revisión y reforma de nuestro marco normativo actual, para responder a las demandas tecnológicas que trae la era digital.

Por otra parte, desde una óptica técnica los ingenieros informáticos del Poder Judicial perciben que, si bien existe una regulación Constitucional y de leyes como la Ley de Protección de Datos Personales. Sin embargo, su aplicación es parcial y centralizada, por lo que debería descentralizarse a fin de cautelar los datos en cada sede judicial.

También se les consulto sobre los protocolos que se utilizan en el Poder Judicial para garantizar el derecho a la autodeterminación informativa; y estos mencionan que la normativa no se cumple en todas las sedes, lo cual se evidencia, por ejemplo, en la existencia de un único oficial de seguridad digital con sede en Lima.

En esa misma línea, se consultó a los ingenieros informáticos sobre cómo se ha venido aplicando la normativa en protección de datos personales en el Poder Judicial; ellos

señalan que los protocolos actuales se centran en el acceso a información solo por parte de quienes están directamente involucrados en un proceso judicial, y que las contraseñas y sistemas se actualizan periódicamente según las directivas del nivel central es decir Lima.

No obstante, reconocen que estos protocolos no siempre se aplican con rigurosidad, lo que debilita la protección del derecho en la práctica cotidiana judicial.

A nivel doctrinario y jurisprudencial, estos hallazgos se alinean con lo desarrollado por Linares (2019), quien reconoce que el derecho a la autodeterminación informativa brinda al titular poderes concretos como el acceso, corrección, supresión y renovación de información, así como la actualización y cambio de datos, funciones que requieren mecanismos efectivos de implementación tanto normativa como tecnológica.

Asimismo, el Tribunal Constitucional peruano ha sostenido como señala García (2014) que los derechos fundamentales deben interpretarse bajo principios como el pro homine, el control de convencionalidad y la protección de derechos implícitos conforme al artículo 3 de la Constitución. Esta interpretación amplia es importante, para enfrentar los desafíos que impone la digitalización. En la interpretación comparada, la tesis de Pérez et al. (2019) revela un fenómeno similar: la existencia de leyes específicas que, no obstante, dejan zonas grises sin regulación, lo que obliga a pensar en marcos legales más integrales.

Asimismo, Díaz (2021) advierte que las acciones constitucionales como el hábeas data, aunque útiles, no siempre ofrecen una reparación efectiva, ni sanciones contundentes ante el uso indebido de datos con fines comerciales.

Del análisis de las entrevistas realizadas a magistrados del Poder Judicial de Apurímac y a ingenieros del área de soporte informático, en contraste con la normativa vigente y la jurisprudencia del Tribunal Constitucional, se establece que la protección de los

datos personales generales frente a la era digital en el sistema constitucional peruano se sustenta en el artículo 2 inciso 6, que protege implícitamente el derecho a la autodeterminación informativa. Asi también, la protección de datos generales se encuentra desarrollado por la Ley N° 29733 y su Reglamento D.S. 016-2024-JUS.

Sin embargo, al analizar de qué manera se protegen efectivamente estos datos, se identifican limitaciones, ya que, los ingenieros entrevistados señalaron que, si bien existen controles de acceso, autenticación y cifrado en los sistemas judiciales, estos resultan insuficientes ante el volumen y velocidad de tratamiento de datos que impone la era digital.

Por otro lado, los magistrados coincidieron en que el proceso de hábeas data, es el principal mecanismo de tutela, presenta dificultades de celeridad en contextos digitales, especialmente en redes sociales y plataformas internacionales.

Este análisis permite advertir que, aunque el marco normativo reconoce la protección de los datos personales generales, y que la era digital ha generado una brecha entre el reconocimiento formal del derecho y su garantía poco efectiva, debido a insuficiencias en infraestructura tecnológica, protocolos de seguridad y capacitación del personal judicial.

Dicha situación genera una tensión en el núcleo esencial de la autodeterminación informativa, pues el control sobre los datos personales que ampara la Constitución no se materializa plenamente cuando las herramientas tecnológicas del Estado no responden a las exigencias de la sociedad de la información.

5.4.2.2 Explicar de qué manera se encuentran protegidos los datos sensibles frente a la era digital en el sistema constitucional peruano.

De los resultados obtenidos se logró determinar que la protección de los datos sensibles frente a la era digital en el sistema constitucional peruano presenta reconocimiento normativo específico, aunque con retos de efectividad en su implementación práctica.

Desde la óptica de los magistrados, se admite que el ordenamiento jurídico nacional tutela los datos sensibles implícitamente mediante el artículo 2 inciso 6 de la Constitución, que consagra la autodeterminación informativa, y mediante la Ley N.º 29733, cuyo artículo 2 numeral 5 conceptualiza como datos sensibles los relacionados a origen racial, salud, vida sexual y convicciones religiosas, asignándoles una protección reforzada.

Sin embargo, los operadores de justicia concuerdan en que este marco normativo se encuentra fragmentado y carece de un cuerpo unificado específico para afrontar los peligros que la era digital representa para la información sensible del ciudadano.

El juez 1 manifestó que la protección de datos sensibles se regula de modo implícito en el marco constitucional. Por su parte, el juez 2 destacó que el Decreto Supremo N.º 029-2021-PCM, Reglamento de la Ley de Gobierno Digital, contempla directrices de seguridad y gestión de identidad digital aplicables al tratamiento estatal de datos sensibles. A su vez, el magistrado 4 reconoció que la regulación continúa siendo dispersa y sin enfoque unificado, lo que incide en la efectividad del sistema de protección legal.

En contraposición, el magistrado 3 sostuvo críticamente que no existe norma integral que regule de forma específica la protección de datos sensibles en entornos digitales, pese a que derechos como la privacidad e intimidad requieren reinterpretación en este contexto tecnológico.

De las manifestaciones de los magistrados se colige que la protección de datos sensibles tiene base formal en el artículo 2 numeral 6 de la Constitución, la Ley N.° 29733

y su reglamento. De igual modo, en los últimos siete años el Estado ha ido emitiendo políticas de transformación digital que, aunque orientadas a modernizar la administración pública, conllevan a una futura recopilación, tratamiento y uso masivo de datos personales, incluidos los sensibles, lo cual puede restringir el control del titular. Entre ellas figuran: el Decreto Legislativo N° 1412 (2018); el Decreto de Urgencia N° 006-2020; el Decreto de Urgencia N° 007-2020; el Decreto Supremo N° 029-2021-PCM; el Decreto Supremo N° 085-2023-PCM; y la Ley N° 31814 (2023).

Actualmente existen seis disposiciones legales asociadas a la era digital, enfocadas principalmente en adecuar servicios públicos y privados. No obstante, ello puede vulnerar el derecho fundamental a la autodeterminación informativa en su vertiente de datos sensibles si los mecanismos vigentes no se ajustan al contexto digital. Tal como indica el magistrado 3, se requiere una norma integral complementaria a la Ley N° 29733, con énfasis en datos sensibles.

Al consultar a los magistrados sobre la influencia de la transformación digital en la interpretación de derechos fundamentales, coincidieron en que la revolución digital ha aumentado la fragilidad de la intimidad y el derecho al olvido, al elevar la difusión de información personal sensible. El Juez 2 aludió al derecho al anonimato como garantía digital para resguardar datos sensibles. Los magistrados 3 y 4 aciertan en que la digitalización ha impactado negativamente al reducir el control efectivo sobre datos personales sensibles.

En el aspecto técnico, los ingenieros de soporte informático del Poder Judicial de Apurímac y Cusco señalaron el uso de directorios activos, firewalls, proxy, cifrado y controles de acceso jerárquicos. Dichos mecanismos buscan salvaguardar la confidencialidad de datos judiciales sensibles conforme a la Ley de Protección de Datos

Personales. Sin embargo, admiten que la ciberseguridad centralizada en Lima limita la respuesta regional ante amenazas a información sensible. Añaden que Blockchain y herramientas Reg Tech se emplean de forma restringida, sin integración plena.

En doctrina, Canizales (2021) advierte que el avance tecnológico coloca a las personas en situación de vulnerabilidad ante el uso indebido de datos sensibles, y que la ausencia de legislación integral sobre tecnologías disruptivas impide protección completa.

Apaza (2023) evidencia que el hábeas data ha servido para tutelar la intimidad frente a datos sensibles ante vacíos legales.

Pérez (2018) afirma que la seguridad de los datos sensibles es pilar de los derechos de la era digital que el constitucionalismo moderno debe incorporar. El caso Facebook, referido por Villar (2019), demuestra que la manipulación de datos sensibles genera efectos políticos y sociales graves, sobre todo en contextos electorales.

En consecuencia, al explicar de qué manera se encuentran protegidos los datos sensibles frente a la era digital, se verifica que existe marco constitucional y legal de tutela reforzada, pero su efectividad se ve afectada por fragmentación normativa, tratamiento masivo de datos impulsado por la transformación digital estatal, centralización de la ciberseguridad, y una débil integración tecnológica en sedes judiciales. Ello produce una brecha entre el reconocimiento formal y la garantía material del control sobre datos sensibles, requiriendo actualizar el hábeas data e implementar protocolos específicos de anonimato y consentimiento cualificado en entornos digitales.

5.4.2.3 Objetivo Especifico 3

Determinar cómo se regula el consentimiento informado frente a la era digital en el sistema constitucional peruano.

Los hallazgos obtenidos a través de entrevistas realizadas a magistrados civiles con competencia constitucional e ingenieros del soporte informático de los Órganos Jurisdiccionales de Apurímac y Cusco, se pudo determinar que la regulación del consentimiento informado frente a la era digital en el sistema constitucional peruano cuenta con previsión normativa, pero demanda fortalecimiento operativo y cultural para alcanzar eficacia plena.

Desde la esfera jurisdiccional, al consultar a los jueces **¿Qué mecanismos pueden adoptarse para proteger el derecho fundamental a la autodeterminación informativa frente a la era digital?**, se evidenció una coincidencia entre la perspectiva jurídica y técnica acerca de la importancia de consolidar los mecanismos relacionados con el consentimiento informado. Los magistrados destacan que el sistema constitucional debe asegurar el acceso y efectividad del hábeas data, instrumento que protege de manera directa la expresión del consentimiento, sobre todo en supuestos de entidades con repositorios de datos en el exterior del país, donde aparecen obstáculos jurisdiccionales para rectificar o suprimir información tratada sin consentimiento válido.

De igual forma, los jueces entrevistados reconocen que un elemento clave para resguardar este derecho consiste en actualizar la legislación adecuándola a los desafíos de la inteligencia artificial y el Big Data, fenómenos que debilitan la libertad de elección al predecir y manipular conductas, incidiendo directamente en la validez del consentimiento informado. El magistrado 3 resalta la urgencia de fijar regulaciones precisas sobre el uso de

datos, con énfasis en el consentimiento informado, indicando que debe comunicarse el alcance del tratamiento de datos personales, de modo que el ciudadano pueda autorizar, rechazar o solicitar modificaciones en el uso de su información, e incluso revocar dicho consentimiento posteriormente.

El juez 2 plantea la implementación de agentes de seguridad de información personal en cada entidad que gestione datos sensibles, figura vinculada al artículo 37 del Reglamento de la Ley N° 29733 respecto al Oficial de Datos Personales, encargado de supervisar el cumplimiento del consentimiento informado. A su turno, el magistrado 4 propone un enfoque integral que articule medidas legales, regulatorias, tecnológicas y educativas, mientras que el juez 1 remarca la solidez del hábeas data como vía judicial para tutelar la revocatoria del consentimiento.

Al preguntar **¿Cómo puede fomentarse una cultura de protección de datos y el derecho fundamental a la autodeterminación informativa en la sociedad peruana?,** todos los magistrados sostienen que debe impulsarse desde la educación formal y campañas masivas de sensibilización. El juez 1 propone sanciones más drásticas a entidades infractoras que procesen datos sin consentimiento. El juez 2 sugiere incorporar la enseñanza de derechos ARCO (acceso, rectificación, cancelación y oposición), desde etapas escolares, prerrogativas que se ejercen justamente cuando el consentimiento ha sido viciado o retirado.

El magistrado 4 plantea incluir estos contenidos en la malla curricular escolar, y el magistrado 3 enfatiza la necesidad de informar a la población sobre riesgos del entorno digital para que su consentimiento sea realmente informado.

En el ámbito técnico, al consultar a los ingenieros informáticos **¿Qué buenas prácticas o medidas de seguridad se recomiendan para fortalecer la protección de los**

datos personales en los sistemas judiciales?, manifestaron la urgencia de elevar la cultura digital institucional, comenzando por no compartir credenciales, ni contraseñas y modificarlas periódicamente, prácticas que garantizan que el tratamiento de datos se efectúe únicamente bajo consentimiento válido del titular. Advierten sobre conductas inseguras extendidas y el empleo de claves débiles, situaciones que comprometen la validez del consentimiento al permitir accesos no autorizados. Subrayan además como esenciales la actualización de sistemas, el cifrado, la implementación de firewalls robustos y planes de respuesta a incidentes, medidas que contribuyen a evitar tratamientos no consentidos de fichas RENIEC o expedientes judiciales.

No obstante, también revelan limitaciones estructurales que repercuten en el consentimiento informado: la gestión de ciberseguridad centralizada en Lima dificulta respuestas ágiles en regiones como Abancay y Cusco frente a vulneraciones que involucren datos tratados sin consentimiento. Aunque existen plataformas de transparencia y casillas electrónicas, no se han consolidado iniciativas locales permanentes que refuercen el control del titular sobre su información.

Estos resultados guardan coherencia con Chura (2022), quien advierte que gran parte de la población desconoce los riesgos asociados a la digitalización de sus datos y que, sin regulación clara sobre consentimiento informado, otros derechos como la privacidad resultan afectados. Pérez (2018) cataloga la seguridad del consentimiento informado como esencia de los derechos humanos de la tercera generación, y demandan regulación especializada ante la complejidad digital.

En tal sentido, al determinar cómo se regula el consentimiento informado frente a la era digital, se verifica que el ordenamiento peruano lo contempla en la Ley N° 29733 y su Reglamento, pero su efectividad se ve restringida por la ausencia de mecanismos específicos

para otorgar y revocar consentimiento en contextos de IA y Big Data, obstáculos jurisdiccionales en bases de datos extranjeros, una débil cultura digital ciudadana respecto a derechos ARCO, y la centralización de la ciberseguridad que merma el control del titular.

Ello impone evolucionar hacia un consentimiento granular, dinámico y revocable, complementado con educación digital y fiscalización preventiva a través de Oficiales de Datos Personales.

5.5. Triangulación de datos. - Derecho a la autodeterminación informativa y la era digital en el sistema constitucional peruano.

5.5.1. Fuentes y Enfoques

Tabla 5: Cuadro de fuentes y enfoques

Fuentes	Perspectiva de análisis.	Principales Hallazgos
Sentencias del Tribunal Constitucional (TC)	Jurisprudencial	Datos personales: El TC dice que sí existe el derecho a controlar nuestros datos. Datos sensibles: Protege con más fuerza cosas como el teléfono o antecedentes policiales. Consentimiento: Dice que el hábeas data es lento cuando una empresa de otro país usa tus datos sin permiso.
Leyes sobre datos personales y gobierno digital.	Enfoque Normativo	Datos personales: El art. 2 inc. 6 de la Constitución y la Ley 29733 dicen que podemos controlar nuestros datos. Datos sensibles: La Ley 29733 dice que datos como salud, religión o raza tienen protección especial. Consentimiento: La Ley 29733 dice que para usar tus datos te deben pedir permiso, pero las leyes de transformación digital como el D.L. 1412 hacen que el Estado use muchos datos a la vez y eso choca con el permiso.
Entrevistas a jueces y magistrados.	Enfoque constitucional y doctrinal	Datos personales: Dicen que el hábeas data es muy lento cuando se trata de Facebook u otras redes. Datos sensibles: Dicen que en internet es más fácil que se filtre nuestra intimidad y datos delicados. Consentimiento: Dicen que la gente ya no tiene control real porque el Estado usa programas automáticos para procesar datos.

Fuentes	Perspectiva de análisis.	Principales Hallazgos
Entrevistas a ingenieros del Poder Judicial.	Enfoque técnico	Datos personales: Usan firewalls y claves, pero igual no alcanza por la cantidad de datos que hay ahora. Datos sensibles: Tienen controles para que solo algunos vean datos delicados, pero todo se maneja desde Lima y eso demora la respuesta en Cusco o Abancay. Consentimiento: No tienen programas que revisen si de verdad la persona dio permiso para usar sus datos en el sistema judicial.
Normativa legal vigente.	Enfoque legal integral.	Datos personales: Constitución, Ley 29733, Reglamento nuevo D.S. 016-2024-JUS. Datos sensibles: La Ley 29733 tiene una parte especial solo para datos sensibles. Consentimiento: El art. 5 de la Ley 29733 dice que el permiso es la regla, pero la Ley de IA N° 31814 permite usar muchos datos y eso complica el permiso. Problema: Hay muchas leyes pero están separadas y no alcanzan para los problemas nuevos de internet.

5.5.2. Esquema resumen de triangulación.

Tabla 6: Esquema de resumen de triangulación

Tema	Normativa y doctrina.	Jurisprudencia	Entrevistas a jueces.	Entrevistas a ingenieros.
Reconocimiento del fundamental a la autodeterminación informativa.	La Constitución art. 2 inc. 6, la Ley 29733 y el Reglamento D.S 016-2024-JUS dicen que podemos controlar nuestros datos personales.	El TC en los casos 0239-2021 y 01116-2022 dijo que sí existe el derecho a la autodeterminación informativa.	Los jueces explican que por este derecho la gente puede controlar sus datos personales.	Los ingenieros dicen que proteger los datos sirve para cuidar la privacidad y que la información del Poder Judicial se use bien.
Vacíos normativos frente a la era digital	Las leyes sobre IA, gobierno y transformación digital regulan servicios públicos, pero no son claras.	Las sentencias muestran que el hábeas data es muy lento, sobre todo en Facebook y páginas de otros países.	Los jueces dicen que las leyes de ahora no alcanzan y hay que hacer reformas para regular la IA, redes sociales y trabajar con otros países.	Los ingenieros dicen que falta poner en práctica todas las reglas de seguridad y que muchos trabajadores judiciales no saben bien cómo proteger los datos.

Protección de datos personales.	La Ley N°29733 dice que para usar tus datos te deben pedir permiso, y tú tienes derechos ARCO: acceder, corregir, borrar u oponerte.	El TC protege datos sensibles como tu número de teléfono o antecedentes policiales cuando se usan mal.	Los jueces dicen que el hábeas data es la herramienta principal para defender tus datos personales.	Los ingenieros dicen que sí tienen controles de acceso, claves y cifrado, pero igual no es suficiente.
Conflictos entre derechos fundamentales.	Las leyes tratan de que haya equilibrio entre tu privacidad, la libertad de expresión y tu derecho a controlar tus datos.	Los casos de Facebook y SIDPOL muestran que choca la privacidad con la libertad de información y con la seguridad del Estado.	Los jueces ven que hay conflictos entre tu derecho a controlar tus datos y la libertad de expresión e información.	Los ingenieros dicen que hay riesgo de que alguien de adentro filtre información o que entren de afuera sin permiso.
Deficiencias del proceso de habeas data	El Código Procesal Constitucional regula el hábeas data, pero no contempla contextos con problemas de internet con empresas de otros países.	El caso de Facebook mostró que es difícil notificar a la empresa y que cumpla la sentencia cuando está en otro país.	Los jueces dicen que el hábeas data ya no es rápido como antes y necesita cambios para que sea más eficaz.	Los ingenieros dicen que como todo se maneja desde Lima y falta buena infraestructura, es difícil proteger los datos rápido.
Ciberseguridad y tecnología	Las leyes de Gobierno en materia digital promueven la digitalización de información de los administrados.	Las sentencias dicen que hay que evitar que se filtren datos del Estado o que alguien entre sin permiso a sus bancos de datos.	Los jueces piden que haya más supervisión y que las reglas para internet sean iguales para todos.	Los ingenieros recomiendan usar firewalls, cifrado, doble clave y controlar bien quién entra a ver los datos.
Necesidad de reformas y políticas públicas.	Las leyes nuevas hablan de "constitucionalismo digital", pero todavía hay vacíos.	El TC poco a poco va ampliando la protección del derecho a controlar tus datos con sus interpretaciones.	Los jueces piden cambiar las leyes, mejorar el hábeas data, regular la IA y coordinar con otros países.	Los ingenieros piden capacitar a la gente, que la seguridad no sea solo en Lima y que haya más presupuesto de inversión en ciberseguridad.

5.5.3. Textos Desarrollados por Áreas

A. Desde la Jurisprudencia (Tribunal Constitucional)

El Tribunal Constitucional garantiza el derecho a la autodeterminación informativa en la medida en que reconoce su protección constitucional, aunque en la práctica enfrenta vacíos normativos y dificultades en la aplicación efectiva del habeas data. En fallos como el N° 01163-2022-PHD/TC, se reafirma que el contenido publicado en redes sociales, especialmente en plataformas como Facebook, no constituye un banco de datos en los términos de la ley, limitando así la protección del derecho. De igual modo, en el Exp. N° 0239-2021-PHD/TC, el Tribunal protege datos sensibles como números telefónicos, exigiendo que exista justificación razonable para su tratamiento. Sin embargo, en ambos casos se evidencia que el hábeas data resulta lento e ineficaz cuando se reclama contra empresas extranjeras que tratan datos sin consentimiento válido. Ello evidencia la necesidad de actualizar la regulación para ampliar los mecanismos efectivos de protección frente a la digitalización y garantizar permisos claros en entornos tecnológicos.

B. Desde las entrevistas a jueces y magistrados

Los magistrados civiles de Abancay coinciden en que el sistema legal vigente no es suficiente para proteger el derecho a la autodeterminación informativa frente a las nuevas tecnologías y los desafíos que impone la era digital. Reconocen la existencia de vacíos en la normativa, en especial respecto a la protección en redes sociales, inteligencia artificial y sistemas transfronterizos. Los jueces manifiestan que la lentitud del proceso judicial y la dispersión normativa dificultan la protección efectiva de los datos personales generales, mientras que advierten mayor fragilidad de la intimidad y de los datos sensibles en entornos digitales. En ese sentido, el juez 2 propone reconocer el derecho al anonimato como garantía digital. Asimismo, indican que el consentimiento informado se debilita por el tratamiento automatizado de datos en servicios públicos digitales, por lo que proponen reformas urgentes

y mecanismos complementarios que exijan permisos claros, revocables y específicos en contextos de IA y Big Data.

C. Desde las entrevistas a ingenieros del Poder Judicial

El análisis revela que las políticas actuales en ciberseguridad y protección de datos son insuficientes, con limitaciones en infraestructura y capacitación. Si bien existen firewalls y cifrado para resguardar datos personales, estos resultan insuficientes ante el volumen y velocidad del tratamiento digital. En cuanto a los datos sensibles, aunque cuentan con controles de acceso diferenciados, la centralización en Lima limita respuestas rápidas en regiones como Cusco y Abancay ante posibles filtraciones. Los ingenieros también señalan que no existen herramientas técnicas que verifiquen si el consentimiento informado es válido antes de procesar datos en los sistemas judiciales. Por ello, recomiendan fortalecer políticas con tecnologías más robustas como autenticación multifactor y Blockchain para garantizar la trazabilidad del permiso, además de promover campañas de sensibilización para cambiar la cultura institucional y ciudadana en protección de datos.

D. Desde el análisis normativo.

El derecho fundamental a la autodeterminación informativa constituye una manifestación moderna del derecho a la dignidad humana en un entorno digital. En el sistema constitucional peruano, este derecho se encuentra sustentado en el artículo 2 inciso 6 de la Constitución Política, que reconoce la protección de los datos y limita su tratamiento arbitrario. A ello se suma la Ley N° 29733, cuyo artículo 2 regula los datos personales generales y cuyo artículo 2 inciso 5 define los datos sensibles otorgándoles un régimen reforzado, aunque disperso. El artículo 5 de la misma ley establece el consentimiento como principio rector. Sin embargo, el avance de las tecnologías digitales y el proceso de transición a un “Gobierno Digital”, impulsado por normas como el D.L. 1412, el D.U. 006-2020, el D.S. 029-2021-PCM y la Ley N° 31814, han obligado al Estado a desarrollar un marco

normativo orientado a la eficiencia, que promueve el tratamiento masivo de datos. En ese contexto, las normas analizadas permiten comprender cómo el ordenamiento jurídico busca equilibrar el desarrollo tecnológico con la protección de los derechos fundamentales. No obstante, la normativa actual se encuentra dispersa y no establece figuras procesales ágiles que garanticen una adecuada protección de datos personales, ni regula de forma clara el consentimiento informado en entornos automatizados, lo que desnaturaliza el permiso al asumirlo tácito o con un “Clic”.

personales.

5.5.4. Triangulación de datos según las categorías y los objetivos planteados:

Objetivo General: Analizar la protección legal del derecho fundamental a la autodeterminación informativa frente a la era digital en el sistema constitucional peruano.

Del análisis integrado de la jurisprudencia, el marco normativo, las entrevistas y la doctrina, se determina que el derecho a la autodeterminación informativa cuenta con reconocimiento constitucional, pero presenta una tutela limitada frente a la era digital. El Tribunal Constitucional vincula este derecho con los entornos tecnológicos, aunque sus pronunciamientos revelan que el hábeas data resulta insuficiente ante plataformas internacionales. Las disposiciones de transformación digital, como el Decreto Legislativo N° 1412 y la Ley N° 31814, fomentan el tratamiento masivo de datos y generan tensión con la protección constitucional. Los magistrados entrevistados sostienen que el ordenamiento jurídico requiere adecuación normativa ante el avance tecnológico. Los ingenieros del Poder Judicial confirman que las políticas de ciberseguridad presentan deficiencias. En síntesis, las fuentes concuerdan en que existe una brecha entre el reconocimiento legal del derecho y su garantía efectiva en el entorno digital.

Objetivo Especifico 1: Explicar de qué manera se protegen los datos personales generales frente a la era digital en el sistema constitucional peruano.

Se establece que los datos personales generales gozan de protección formal, pero con eficacia limitada en el ámbito digital. El artículo 2 inciso 6 de la Constitución y la Ley N° 29733 consagran el derecho a controlar los datos personales. No obstante, el Tribunal Constitucional, en el Exp. N° 01116-2022-PHD/TC, determinó que las publicaciones en Facebook no constituyen banco de datos, restringiendo la tutela del hábeas data en redes sociales. Los jueces manifiestan que dicho proceso constitucional carece de celeridad frente a plataformas internacionales, quedando los datos personales expuestos. Los ingenieros precisan que los mecanismos de firewall y cifrado resultan insuficientes ante el volumen actual de información. La doctrina, según Linares (2019), señala que la legislación no contempló escenarios digitales. Por tanto, la protección de los datos personales se encuentra prevista en la norma, pero desprovista de eficacia práctica en internet.

Objetivo específico 2: Explicar de qué manera se encuentran protegidos los datos sensibles frente a la era digital en el sistema constitucional peruano.

Se constata que los datos sensibles cuentan con un régimen de protección reforzada en el ordenamiento jurídico, aunque con debilidades operativas en el entorno digital. El artículo 2 inciso 5 de la Ley N° 29733 otorga mayor resguardo a datos de salud, religión y vida sexual. El Tribunal Constitucional, en el Exp. N° 0239-2021-PHD/TC, exige justificación especial para su tratamiento. Los magistrados advierten mayor vulnerabilidad de la intimidad en internet y proponen el derecho al anonimato como garantía digital. Los ingenieros indican que los datos sensibles poseen controles de acceso diferenciados, pero la centralización en Lima impide respuestas oportunas en sedes regionales ante filtraciones. El Decreto de Urgencia N° 007-2020 creó el Centro Nacional de Seguridad Digital, cuya

implementación es aún incipiente. En consecuencia, existe protección normativa y jurisprudencial reforzada, pero con limitaciones en su aplicación práctica.

Objetivo específico 3: Determinar cómo se regula el consentimiento informado frente a la era digital en el sistema constitucional peruano.

Se verifica que el consentimiento informado se encuentra regulado como principio rector, pero presenta desnaturalización en la práctica digital. El artículo 5 de la Ley N° 29733 exige consentimiento previo, expreso e informado para el tratamiento de datos. Sin embargo, las normas de gobierno digital admiten tratamientos masivos mediante el "Click" o aceptación tácita, contraviniendo dicho principio. El Tribunal Constitucional evidenció que el hábeas data carece de eficacia para exigir consentimiento válido frente a empresas extranjeras como Facebook. Los jueces señalan que el tratamiento automatizado en servicios públicos digitales reduce el control efectivo del titular y proponen reformas para garantizar consentimiento granular y revocable. Los ingenieros confirman la inexistencia de herramientas que verifiquen la validez del consentimiento previo al procesamiento de datos.

Conforme a Canizales (2021), la aceptación de términos extensos sin lectura efectiva anula el consentimiento. Por ello, la regulación del consentimiento no se adecúa a las dinámicas de la era digital.

5.5.5. Conclusión de la Triangulación

Desde mi perspectiva, se infiere que el derecho a la autodeterminación informativa está reconocido en el sistema constitucional peruano, pero su tutela es limitada frente a la era digital. Si bien el hábeas data lo protege formalmente, resulta lento e ineficaz en entornos digitales, especialmente con datos personales, datos sensibles y consentimiento informado.

Las políticas técnicas del Poder Judicial son insuficientes y la normativa vigente está dispersa, por lo que se requiere una reforma legal integral, modernización tecnológica y educación digital para garantizar una protección efectiva de este derecho.

VI. Conclusiones

Primero. – Analice y determine de mi investigación que el marco constitucional peruano reconoce el derecho fundamental a la autodeterminación informativa en el contexto digital. No obstante, su efectividad se ve limitada frente a los retos tecnológicos y las trabas procesales existentes.

Asi también, entre los principales obstáculos del sistema judicial nacional se identificó la escasa formación de los jueces en materia digital y la inexistencia de normativa específica y vigente que regule fenómenos emergentes como el procesamiento masivo de datos.

A esto se suma que la jurisprudencia reciente del Tribunal Constitucional ha establecido límites a la protección, particularmente en casos sobre redes sociales. Se ha señalado que las cuentas personales no califican como bancos de datos bajo la Ley de Protección de Datos Personales, lo que genera controversia sobre el alcance real de este derecho en plataformas digitales.

Asimismo, el hábeas data, concebido constitucionalmente como un proceso sumario, en la práctica resulta extenso y de baja eficacia. Esto se agrava cuando la información está en poder de corporaciones extranjeras, situación que complica las notificaciones y el cumplimiento de resoluciones judiciales.

Desde una perspectiva técnica, el Poder Judicial presenta falencias en la gestión de datos; protocolos de seguridad deficientes, débil cultura institucional en privacidad y déficit de especialistas en ciberseguridad, factores que impiden aplicar políticas efectivas de protección.

Segundo. - Se establece que los datos personales generales poseen un reconocimiento formal en el ordenamiento peruano, a través del artículo 2 inciso 6 de la Constitución y la Ley N° 29733. La doctrina del Tribunal Constitucional refleja que el hábeas data no ofrece una tutela

real de datos personales generales en redes sociales, tal como se precisó en el análisis del Exp. N° 01116-2022-PHD/TC al indicar que Facebook no constituye un banco de datos.

Los operadores de justicia entrevistados coinciden en que el procedimiento resulta lento y poco viable frente a empresas transnacionales. Por otro lado, los especialistas en sistemas del Poder Judicial advierten que los mecanismos actuales de firewall y encriptación son insuficientes ante el flujo masivo de información. En consecuencia, si bien la protección existe a nivel normativo, no logra concretarse en los entornos tecnológicos.

Tercero. – En cuanto, a los datos sensibles, se concluye que cuentan con un marco de protección reforzada según el artículo 2 inciso 5 de la Ley N° 29733 y el criterio del Tribunal Constitucional en el Exp. N° 0239-2021-PHD/TC, que requiere una justificación cualificada para su tratamiento. Pese a ello, en la práctica digital se presentan serias deficiencias operativas.

Los jueces entrevistados destacan una mayor exposición del derecho a la intimidad y plantean incorporar el derecho al anonimato como resguardo en entornos digitales. Los ingenieros institucionales señalan que, aunque existen accesos diferenciados, la centralización administrativa en Lima dificulta una respuesta inmediata ante incidentes de seguridad en otras regiones. En consecuencia, la protección de datos sensibles es sólida en la ley, pero frágil en su aplicación práctica.

Cuarto. - El consentimiento informado está regulado como núcleo central en el artículo 5 de la Ley N° 29733, exigiendo autorización previa, expresa e informada del titular.

No obstante, este consentimiento se desvirtúa en el contexto digital, ya que, las normas sobre gobierno digital como la Ley N° 31814 de Inteligencia Artificial permiten tratamientos masivos basados en el “clic" o aceptación implícita.

Los magistrados indican que el procesamiento automatizado en la administración pública disminuye el control efectivo del titular y proponen implementar modalidades de

consentimiento revocable. Desde el área técnica, se confirma la falta de mecanismos que validen la legitimidad del consentimiento antes del tratamiento de datos.

En síntesis, la regulación vigente sobre consentimiento no responde adecuadamente a las dinámicas tecnológicas actuales.

VII. Recomendaciones

Primero. – A fin de garantizar el ejercicio efectivo del derecho a la autodeterminación informativa, corresponde fortalecer los protocolos de ciberseguridad en las instituciones públicas y privadas que gestionan bases de datos, incorporando responsables especializados en protección de datos en cada entidad, conforme a lo previsto en el marco del artículo 37 del Reglamento de la Ley N° 29733.

Se precisa que el actual Reglamento de Protección de Datos Personales no detalla en qué organismos debe implementarse dicha figura. No obstante, ante el avance acelerado de la tecnología, resulta prioritario que esta incorporación se efectúe de manera inmediata y en todo el territorio nacional, sin distinguir el tipo de información administrada.

En el sistema judicial, es necesario impulsar programas de formación continua para jueces, auxiliares jurisdiccionales y servidores públicos, orientados a desarrollar competencias en materia tecnológica y asegurar una aplicación coherente de la normativa sobre datos personales.

Bajo ese sentido, se requiere consolidar un marco legal específico y actualizado que atienda los nuevos retos digitales, evitando la fragmentación normativa existente. Dicha regulación debe alinearse con los postulados constitucionales y contemplar herramientas jurídicas eficaces para supuestos que involucren corporaciones extranjeras y flujo transfronterizo de datos, viabilizando la notificación y ejecución de resoluciones en dichos casos.

Segundo. – En cumplimiento de su obligación de legislar, corresponde al Congreso integrar en la Ley N° 29733 disposiciones específicas sobre la protección de datos personales en redes sociales y entornos digitales. Se plantea habilitar un proceso de hábeas data digital con carácter sumarísimo, que alcance a compañías extranjeras, aunque carezcan de domicilio en el Perú. Asi también, el sistema de justicia debe contar con mecanismos para notificar y

sancionar directamente a plataformas como Facebook cuando afecten datos de ciudadanos peruanos, superando así el criterio jurisprudencial que las excluye de la categoría de bancos de datos.

Tercero. - El Poder Judicial debe crear Unidades de Ciberseguridad Descentralizadas en todas las Cortes Superiores, con personal técnico permanente que atienda incidentes de filtración de datos sensibles a nivel regional. Por ende, se sugiere incorporar al ordenamiento el derecho al olvido digital como protección reforzada para datos vinculados a salud, convicciones religiosas e intimidad personal.

Cuarto. - El Poder Legislativo debe reformar el Reglamento de la Ley N° 29733 a fin de eliminar cualquier modalidad de consentimiento tácito o por "clic" en los servicios estatales digitales.

Es pertinente disponer la exigencia de consentimiento específico por cada finalidad de tratamiento, con posibilidad de revocación en todo momento, especialmente en sistemas de inteligencia artificial bajo la Ley N° 31814. Las políticas de Gobierno Digital deben contemplar en sus plataformas estatales sistemas de validación previa del consentimiento mediante autenticación de doble factor y registros digitales inalterables que garanticen la trazabilidad de la decisión del titular.

En consecuencia, la normativa procesal constitucional debe incluir medidas cautelares especiales para entornos digitales que permitan la suspensión inmediata del tratamiento de datos y la supresión de contenido en plataformas globales. Asimismo, es necesario impulsar alianzas de cooperación internacional que viabilicen el emplazamiento y cumplimiento de sentencias contra empresas tecnológicas con sede fuera del país.

VIII. Referencias

Abad Yupanqui, S. (1992). Límites y respeto al contenido esencial de los derechos fundamentales. Estudio preliminar. Themis: Revista de Derecho, (21), 7-15.

Alexy, R. (1993). Teoría de los derechos fundamentales. Centro de Estudios Constitucionales.

Álvarez, A. J. (2021). El concepto de sistema jurídico (Tesis doctoral, Universitat Pompeu Fabra).

Apaza Jibaja, E. V. (2023). El acceso a la información y el derecho a la intimidad personal en la demanda de habeas data en el periodo 1998-2016 (Tesis de maestría, Universidad José Carlos Mariátegui). http://repositorio.ujcm.edu.pe/bitstream/handle/20.500.12819/1788/Elizabeth_tesis_grad-acad_2023.pdf

Barrera, E. E. (2004). El habeas Data en el Derecho comparado y el Perú. En E. E. Barrera, Derecho Procesal Constitucional (pp. 245-280). Jurista Editores E.I.R.L.

Canizales Reyes, N. (2021). La eficacia horizontal de los derechos humanos. El caso del derecho a la autodeterminación informativa (Tesis de maestría, Universidad Panamericana). https://scripta.up.edu.mx/bitstream/handle/20.500.12552/6340/222098.pdf

Castillo, T. D. (2018). Retos, riesgos y oportunidades de la sociedad digital. En T. De la Quadra Salcedo & J. L. Piñar Mañas, Sociedad digital y Derecho (pp. 21-86). Boletín Oficial del Estado.

Chura Vargas, R. W. (2022). La necesidad de incorporar la autodeterminación informativa como derecho fundamental en la Constitución Política del Estado (Tesis de licenciatura,

Universidad Mayor de San Andrés). https://repositorio.umsa.bo/bitstream/handle/123456789/31297/TD-5878.pdf

Congreso de la República. (1993). Constitución Política del Perú.

Contreras, P. (2017). Titularidad de los derechos fundamentales. En P. Contreras & C. Salgado, Manual sobre derechos fundamentales. Teoría general (pp. 119-160). LOM Ediciones.

Decreto de Urgencia N.° 006-2020. (2020, 9 de enero). Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. Diario Oficial El Peruano.

Decreto de Urgencia N.° 007-2020. (2020, 9 de enero). Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Diario Oficial El Peruano.

Decreto Legislativo N.° 1412. (2018, 13 de septiembre). Decreto Legislativo que aprueba la Ley de Gobierno Digital. Diario Oficial El Peruano.

Decreto Supremo N.° 016-2024-JUS. (2024, 30 de noviembre). Decreto Supremo que aprueba el Reglamento de la Ley N.° 29733, Ley de Protección de Datos Personales. Diario Oficial El Peruano.

Decreto Supremo N.° 029-2021-PCM. (2021, 19 de febrero). Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N.° 1412. Diario Oficial El Peruano.

Decreto Supremo N.° 085-2023-PCM. (2023, 28 de julio). Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030. Diario Oficial El Peruano.

Díaz Sosa, S. M. (2021). Protección constitucional de habeas data ante acumulación ilegal de información con fines de potenciales negocios (Tesis de maestría, Universidad Nacional José Faustino Sánchez Carrión).

https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/6083/SILVIA%20MILAGROS%20DIAZ%20SOSA.pdf

Fabián Rojas, J. A. (2021). Fundamentos para la incorporación del derecho al olvido en el sistema jurídico constitucional peruano (Tesis de licenciatura, Universidad César Vallejo). https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/80177/Fabian_RJA-SD.pdf

García Toma, V. (2014). Teoría del Estado y Derecho Constitucional. ADRUS D&L Editores S.A.C.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill / Interamericana Editores.

Ingunza, C. (2022, 18 de enero). El caso contra Mark Zuckerberg en el Perú: ¿se puede declarar improcedente de manera liminar una demanda de amparo constitucional? Rafael Prado Litigio Judicial y Arbitral. https://rpb.pe/el-caso-contra-mark-zuckerberg-en-el-peru-se-puede-declarar-improcedente-de-manera-liminar-una-demanda-de-amparo-constitucional/

Landa Arroyo, C. (2017). Los derechos fundamentales. Fondo Editorial PUCP.

Ley N.° 29733. (2011, 3 de julio). Ley de Protección de Datos Personales. Diario Oficial El Peruano.

Ley N.° 31814. (2023, 5 de julio). Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. Diario Oficial El Peruano.

Linares Luna, S. M. (2019). El contenido constitucional del derecho fundamental a la autodeterminación informativa en el Derecho Constitucional Peruano [Tesis de licenciatura, Universidad de Piura].

Manzano Guevara, E. P. (2021). El habeas data y los derechos de protección de los datos personales en Ecuador (Tesis de maestría, Universidad Nacional de Tumbes). https://repositorio.untumbes.edu.pe/bitstream/handle/20.500.12874/2663/TESIS%20-%20MANZANO%20GUEVARA.pdf

Nolasco, E. M. (2024, 2 de noviembre). Caso Interbank: ¿Qué habría detrás de la extorsión y la filtración de datos de clientes por el supuesto 'hacker'? Infobae. https://www.infobae.com/peru/2024/10/31/caso-interbank-filtracion-de-datos-de-millones-de-clientes-se-habria-dado-tras-fallidas-negociaciones-con-extorsionador-digital/

Perelló Oliver, S. (2009). Metodología de la investigación social. Dykinson S.L.

Pérez Erazo, A. U., Sánchez Quintanilla, M. D., & Ventura Morales, E. A. (2019). La regulación del derecho a la autodeterminación informativa en El Salvador [Tesis de licenciatura, Universidad de El Salvador].

Pérez Luño, A. E. (2018). Las generaciones de derechos humanos ante el desafío posthumanista. En T. De la Quadra-Salcedo & J. L. Piñar Mañas, Sociedad digital y Derecho (pp. 137-155). Boletín Oficial del Estado.

Polanco, M. (2020, 20 de enero). Magazcitum. https://www.magazcitum.com.mx/index.php/archivos/5222

Rebollo Delgado, L. (2023). Inteligencia artificial y derechos fundamentales. Dykinson.

RPP. (2017, 10 de agosto). ¿Qué es y qué implicó el caso Petro audios? RPP Noticias. https://rpp.pe/politica/judiciales/que-es-y-que-implico-el-caso-petroaudios-noticia-1069475

Sánchez, D. V. (2024, mayo). Repositorio ESAN. https://repositorio.esan.edu.pe/server/api/core/bitstreams/57cd1aa5-17a0-4250-8fe0-4ae567302d4a/content

Sánchez, H., Reyes, C., & Mejía, K. (2018). Manual de términos en una investigación científica, tecnológica y humanística. Universidad Ricardo Palma. https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion.pdf

Sarrión, J. E. (2023). El reconocimiento y protección de los derechos y libertades en un mundo en transformación. ¿Hacia un nuevo paradigma constitucional? Aranzadi.

Serrano, C. I. (2021). Wikileaks, Anonymous y Snowden, ¿Rebelión legítima? (Trabajo de fin de grado, Universidad Pontificia Comillas). https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/47369/TFG-%20Izquierdo%20Serrano%2C%20Cristina%20.pdf

The Guardian. (2018, 17 de marzo). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Tribunal Constitucional del Perú. (2002, 29 de enero). Expediente N.° 1797-2002-HD/TC. https://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

Tribunal Constitucional del Perú. (2023, 19 de mayo). Expediente N.° 01163-2022-PHD/TC. https://tc.gob.pe/jurisprudencia/2023/01163-2022-HD.pdf

Tribunal Constitucional del Perú. (2020). Expediente N.° 00786-2020-PHD/TC. https://tc.gob.pe/jurisprudencia/2020/00786-2020-HD.pdf

Tribunal Constitucional del Perú. (2021). Expediente N.° 03326-2019-PHD/TC. https://jurisprudencia.sedetc.gob.pe/sentencia/03326-2019-PHD-TC

Tribunal Constitucional del Perú. (2022). Expediente N.° 00696-2021-PHD/TC. https://www.tc.gob.pe/jurisprudencia/2022/00696-2021-HD.pdf

Tribunal Constitucional del Perú. (2023). Expediente N.° 00073-2022-PHD/TC. https://www.tc.gob.pe/jurisprudencia/2023/00073-2022-HD.pdf

Ugarte, P. S. (2015). Sobre el concepto de Constitución. En J. L. Fabra Zamora & E. Spector, Enciclopedia de filosofía y teoría del derecho (Vol. 3, pp. 1930-1958). Instituto de Investigaciones Jurídicas - UNAM.

Vercelli, A. (2018). La (des) protección de los datos personales: análisis del caso Facebook Inc. - Cambridge Analytica. SID, (47), 1-12. https://core.ac.uk/download/pdf/296409059.pdf

Villar Mir, J. M. (2019). Los retos de la era digital. Anales de la Real Academia de Ciencias Morales y Políticas, (96), 241-256.

Viveros Abad, M. (2018). Derecho a la autodeterminación informativa respecto a los datos genéticos (Tesis de maestría, Universidad de Chile). https://repositorio.uchile.cl/bitstream/handle/2250/151550/Derecho-a-la-autodeterminaci%c3%b3n-informativa-respecto-a-los-datos-gen%c3%a9ticos.pdf

Los anexos, panel fotográficos y otros documentos están resguardados en la oficina de repositorio digital institucional en la Biblioteca Central de la Universidad Tecnológica delos Andes.