UNIVERSIDAD ESAN

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

CARRERA DE DERECHO CORPORATIVO

"Reconocimiento biométrico en el Perú: Entre la vigilancia ciudadana y el control laboral"

Trabajo de Suficiencia Profesional presentado en satisfacción parcial de los requerimientos para obtener el título profesional de Abogado

AUTORES

Ascencio Malpica, Claudia Daniela

Lomparte Quiñones, Valeria Lucero

Pajuelo Henostroza, Grecia Carmela

ASESOR

Costa Galvez, Jean Carlo

ORCID N° 0001-7831-5959

Marzo, 2025

Trabajo de Suficiencia Profesional (3).pdf

INFORME DE ORIGINALIDAD

1%	1%	3%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.esan.edu.pe Fuente de Internet	1%
2	hdl.handle.net Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

ÍNDICE DE CONTENIDOS

RESUMEN

En el contexto del desarrollo tecnológico, el reconocimiento biométrico se ha convertido en una herramienta esencial para la identificación de personas en ámbitos como la vigilancia ciudadana y el control laboral. Sin embargo, su uso plantea riesgos significativos para la privacidad y la protección de datos personales, especialmente al tratarse de información sensible. En el ámbito laboral, se implementan tecnologías biométricas, como dispositivos de reconocimiento dactilar, como parte del control laboral, mientras que, en espacios públicos, cámaras con inteligencia artificial facilitan la identificación de sujetos delictivos. Esta investigación explora los límites en el uso de la biometría, evidenciando vacíos normativos que podrían facilitar un tratamiento excesivo de datos personales y afectar los derechos fundamentales. La problemática es especialmente visible en el entorno laboral, donde se exige la identificación biométrica incluso cuando medidas menos invasivas serían suficientes. Por último, se evaluará la legitimidad de estas prácticas, con el fin de establecer mecanismos que equilibren la seguridad y la privacidad sin comprometer las libertades fundamentales.

Palabras clave: protección de datos personales, datos sensibles, datos biométricos, derecho a la intimidad, inteligencia artificial.

ABSTRACT

In the context of technological development, biometric recognition has become an essential tool for identifying individuals in areas such as citizen surveillance and workplace control. However, its use poses significant risks to privacy and the protection of personal data, especially when dealing with sensitive information. In the workplace, biometric technologies, such as fingerprint recognition devices, are implemented as part of labor control, while in public spaces, AI-powered cameras facilitate the identification of criminal suspects. This research explores the limits of biometric use, highlighting regulatory gaps that could enable excessive processing of personal data and impact fundamental rights. The issue is particularly evident in the workplace, where biometric identification is required even when less intrusive measures would suffice. Finally, the legitimacy of these practices will be assessed to establish mechanisms that balance security and privacy without compromising fundamental freedoms.

Keywords: *protection of personal data, sensitive data, biometric data, right to privacy, artificial intelligence.*

CAPÍTULO I: INTRODUCCIÓN

1.1. Descripción de la realidad problemática

En un entorno en constante transformación, la seguridad ha sido una preocupación fundamental para las sociedades a lo largo del tiempo. Inicialmente, la atención se centraba en garantizar la protección física frente a diversas amenazas. Sin embargo, con el avance de la tecnología y la expansión del internet, esta necesidad ha evolucionado, abarcando nuevos ámbitos que exigen repensar los mecanismos tradicionales de resguardo y adaptarlos a los desafíos de la era digital. Siguiendo la teoría de las necesidades de Malinowski, la seguridad se reconoce como una de las siete necesidades básicas del ser humano, abarcando no solo la integridad física, sino también la seguridad informática y la protección de los datos personales en entornos digitales[1].

El avance tecnológico ha permitido la implementación de sistemas de reconocimiento biométrico basados en inteligencia artificial (en adelante IA) en diversos ámbitos, incluyendo la vigilancia ciudadana. En el Perú, el uso de estas tecnologías ha crecido significativamente en los últimos años, planteando desafíos en términos de protección de datos personales y derechos fundamentales. La falta de un marco normativo claro y actualizado genera preocupaciones sobre la posible vulneración del derecho a la autodeterminación informativa de los ciudadanos y trabajadores.

En el sector laboral, muchas empresas y entidades públicas han adoptado sistemas de control de asistencia mediante biometría. Si bien, estos sistemas pueden aumentar la eficiencia y seguridad, también han sido duramente cuestionados ya que podrían vulnerar la autodeterminación informativa y el consentimiento informado de los trabajadores. La utilización de estos sistemas de reconocimiento biométrico para supervisar a los empleados ha generado debates sobre la posible afectación de la privacidad y la dignidad de los trabajadores. Aunque el empleador tiene la facultad de supervisar el desempeño laboral, este control debe ejercerse dentro de límites que respeten los derechos fundamentales del trabajador[2].

---

[1] Laisha Mubarak Aguad, "El internet, el Bigdata y el tratamiento de datos personales". *Advocatus*, no. 36 (2017): 206.

[2] César Alfredo Puntriano Rosas, "La videovigilancia en el ámbito laboral", IX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 19 de febrero, https://www.spdtss.org.pe/wp-content/uploads/2021/10/IX-Congreso-Nacional-full-719-747.pdf?utm_source=chatgpt.com

Los datos biométricos son considerados sensibles y, por lo tanto, su tratamiento requiere del consentimiento expreso del titular y la implementación de medidas de seguridad adecuadas para evitar su uso indebido[3]. Sin embargo, en Perú, la ausencia de una regulación específica ha generado vacíos legales que podrían comprometer la privacidad y seguridad de los ciudadanos. Aunque el reconocimiento biométrico ofrece ventajas en términos de seguridad y eficiencia, su implementación debe realizarse dentro de un marco normativo que garantice la protección de los derechos fundamentales.

Es imperativo establecer regulaciones claras que definan los límites y condiciones de su uso, tanto en el ámbito público como en el privado, asegurando un equilibrio entre los beneficios tecnológicos y la salvaguarda de la dignidad y privacidad de las personas.

Al integrar tecnologías biométricas a las empresas, estas deben de adherirse, en la práctica, a regulaciones estrictas para proteger a los empleados, clientes y ciudadanos. También debe de entrar en materia de discusión las responsabilidades que los dueños de los datos tienen al aplicar estas tecnologías, incluyendo la transparencia, la limitación en base al propósito de su uso y la integridad de los mismos.

Cuando se realizan transferencias de datos personales, está por demás mencionar que los responsables deben informar a los titulares, e igualmente recabar el consentimiento para ello en caso de que el tipo de datos así lo requiera. Por ello se necesita una regulación adecuada ya que “el enfoque humano es clave para que la IA beneficie a las personas. Este progreso promete una identidad digital verificada que impulsa la seguridad, buscando evitar fraudes y mejorando experiencias cotidianas. Así como lo fueron las huellas dactilares, hoy los datos biométricos garantizan mayor seguridad y comodidad global”[4]. Pero sigue siendo muy ambigua su normativa en el Perú, los propietarios de los datos biométricos necesitan tener la certeza de que estos mismos estarán protegidos y serán usados de manera adecuada, obligando así a las empresas a actuar conforme a leyes debidamente establecidas para el manejo de este tipo de datos.

---

[3] Ministerio de Justicia y Derechos Humanos. Opinión consultiva N° 032-2021-JUS/DGTAIPD, de 17 de agosto de 2021, se refiere a los datos biométricos y su empleo en la identificación de personas, el tratamiento de datos personales, la obtención del consentimiento, la conservación de documentos digitales, la atención de derechos ARCO y registro de bancos de datos.

[4] Gabriel Antelo. “De las huellas dactilares a los datos biométricos”. *El Peruano*, 6 de diciembre, 2024. https://elperuano.pe/noticia/259487-de-las-huellas-dactilares-a-los-datos-biometricos

1.2. Problemas de investigación

1.2.1. Problema general

¿De qué manera el uso del reconocimiento biométrico afecta el derecho a la protección de datos personales en el ámbito de la videovigilancia ciudadana y el control laboral? ¿Las instituciones están tomando medidas suficientes para garantizar la autodeterminación informativa de los ciudadanos y trabajadores?

1.2.2. Problemas específicos

a. ¿Cuáles son los principales riesgos que el reconocimiento biométrico plantea para la protección de datos personales y la autodeterminación informativa en la vigilancia ciudadana y el control laboral?

b. ¿Cómo se ha abordado en otros países la regulación sobre la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral? ¿Qué medidas han adoptado para garantizar la protección de los datos personales y la autodeterminación informativa de los ciudadanos?

1.3. Objetivos de investigación

1.3.1. Objetivo general

Determinar cuales son las consecuencias jurídicas derivadas del uso del reconocimiento biométrico en la videovigilancia ciudadana y el control laboral, con el propósito de evaluar su impacto en la protección de datos personales y la garantía del derecho a la autodeterminación informativa.

1.3.2. Objetivos específicos

a. Determinar los principales riesgos jurídicos que genera la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral en el Perú, evaluando su impacto en la protección de datos personales y en el derecho a la autodeterminación informativa.

b. Evaluar de qué manera han abordado otros países la regulación sobre la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral sobre la protección de datos personales.

1.4. Justificación de la investigación

El concepto de biometría ha evolucionado enormemente con el paso en el desarrollo de nuevas tecnologías y son utilizados en diversos ámbitos en la actualidad. Por ejemplo, la biometría se emplea para la identificación de las personas mediante reconocimiento facial o de huellas dactilares, ofreciendo un nivel adicional de seguridad y comodidad para los usuarios. Estas tecnologías no solo agilizan los procesos cotidianos, sino que también ayudan a prevenir delitos al dificultar la suplantación de identidad y el acceso no autorizado a espacios restringidos.

Actualmente, también han sido utilizados en procesos judiciales, donde el análisis de material genético como la sangre, la saliva o el pelo puede ser crucial para determinar la identidad o la culpabilidad de una persona. Otro ejemplo de su uso lo encontramos en el reconocimiento facial que se utiliza en los escáneres de los aeropuertos para mejorar la seguridad y facilitar el control de pasajeros o para desbloqueo de dispositivos móviles, entre otras funciones.

Estos datos también se utilizan como medida de seguridad en sistemas sensibles y en instalaciones de alto riesgo, así como para la vigilancia pública a través de cámaras de seguridad. Además, se aplican en la tecnología bancaria, gubernamental e incluso en la identificación de pacientes en el ámbito médico, demostrando la versatilidad y el potencial de los datos biométricos en la vida cotidiana[5].

Es por eso que es necesario realizar una investigación para saber si existe una adecuada normatividad en el Perú con relación a la protección de este tipo de datos, ya que como vemos es una tecnología que está abarcando tanto a empresas del sector privado como del sector público. Ya que en la actualidad es una práctica común en las empresas y aunque los datos biométricos son más seguros que las contraseñas tradicionales, no son completamente inmunes a las brechas de seguridad. Si una base de datos biométrica es comprometida, los datos robados no pueden ser simplemente cambiados o actualizados como una contraseña. Esto podría tener consecuencias graves para los empleados afectados, ya que los datos biométricos son permanentes y únicos[6].

---

[5] Susan Mender Bini, Sistemas biométricos (Argentina: Editorial Eldial - 2024). 135.
[6] Vanessa Diaz, El ejercicio de los derechos ante el flujo de información biométrica (México: Editorial UNAM - 2016). 25.

El tratamiento de los datos biométricos es un tema delicado, ya que puede vulnerar la privacidad de las personas. Este debería de informarse expresamente mediante instrumentos como el aviso de privacidad, en donde se redacta adecuadamente la o las finalidades para las cuales serán tratados los datos biométricos recabados. Pero en la práctica muchas veces esto no se lleva a cabo. Es necesario el poder garantizar que cada uno de los datos biométricos que vayan a ser procesados sean correctos, estén completos y que sean actuales, y además de esto, poder garantizar que no van a ser conservados por un plazo mayor al estipulado y que serán usados sólo con las finalidades descritas previamente[7]. Y para garantizar todo esto, se necesitan leyes adecuadas que permitan obligar a las empresas a cuidar toda la información biométrica que recaben.

Se busca con esta investigación que se tome conciencia sobre la forma en que los datos biométricos son tratados además de analizar si las medidas de seguridad son las adecuadas tanto en el ámbito administrativo como en el técnico y en el manejo y proceso de la obtención de los mismos para que con esto se pueda garantizar que este tipo de datos se encuentren debidamente protegidos, sean usados sólo con el propósito descrito previamente a su obtención, y vigilar que estos mismos no sean eliminados o que tengan un uso que no esté autorizado. Que las empresas y las instituciones responsables de garantizar la seguridad de estos datos cuenten con un marco legal adecuado para su tratamiento.

[7] Editorial Leto, “Uso de datos biométricos en la oficina”, RH en las empresas, 26 de septiembre de 2024, https://rhenlasempresas.com/2024/09/26/datos-biometrico/

CAPÍTULO II: MARCO TEÓRICO

2.1. El derecho a la protección de datos personales

2.1.1. Marco normativo en materia de protección de datos personales

La Constitución Política del Perú es la norma fundamental del país y constituye la base sobre la cual se estructuran el resto de normas del ordenamiento jurídico. A diferencia del modelo clásico de la pirámide de Kelsen, el sistema normativo peruano reconoce la importancia de la ética, la moral y el reconocimiento de los derechos fundamentales como principios esenciales dentro de su estructura. Estos derechos están consagrados en la Constitución, particularmente en los artículos 1 y 2, y son tutelados por el Estado con el fin de garantizar la dignidad y el bienestar de las personas.

En este contexto, el artículo 2, inciso 6 de la Constitución reconoce el derecho de toda persona a que ningún servicio informático, ya sea público o privado, computarizado o no, proporcione información que vulnere su intimidad personal y familiar. Este precepto constitucional sirvió como fundamento para la creación de un marco normativo específico en materia de protección de datos personales, lo que llevó a la promulgación de la Ley N° 29733 – Ley de Protección de Datos Personales (en adelante LPDP)[8].

Dicha ley reconoce y garantiza una serie de derechos a los titulares de datos personales, como el derecho a ser informados sobre el tratamiento que le darán a su información, el derecho de acceso a sus datos y la posibilidad de oponerse a su uso en determinadas circunstancias. Para ello, la norma establece requisitos, principios y obligaciones que deben cumplir quienes recopilan, almacenan, transfieren o utilizan datos personales, asegurando así su adecuado manejo dentro de un marco legal que busca proteger la privacidad y la autodeterminación informativa de los ciudadanos[9].

---

[8] Moore,*"Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales"*,436-.437.

[9] Autoridad Nacional de Protección de Datos Personales, *El Derecho Fundamental a la Protección de Datos Personales: Guía para el Ciudadano* (Lima: Ministerio de Justicia y Derechos Humanos, 2013), https://cdn.www.gob.pe/uploads/document/file/1401558/El%20derecho%20fundamental%20a%20la%20protecci%C3%B3n%20de%20datos%20personales.pdf.

Desde el surgimiento de la era digital y la expansión del internet, la tecnología ha evolucionado de manera exponencial, transformando distintos aspectos de la sociedad. Hoy en día, vivimos en un mundo cada vez más interconectado, donde el desarrollo de nuevas herramientas digitales y la inteligencia artificial han impulsado avances en áreas como la comunicación, la educación, la salud y el comercio.

Sin embargo, este crecimiento también ha planteado desafíos en materia de privacidad y seguridad de la información. El uso masivo de datos personales ha hecho necesario establecer marcos normativos que regulen su tratamiento y protejan los derechos de las personas en un entorno tecnológico en constante cambio. En este sentido, la Ley N° 29733 define principios fundamentales para garantizar la privacidad, mientras que su reglamento, aprobado mediante el Decreto Supremo N° 003-2013-JUS, establece directrices claras para su aplicación, buscando un equilibrio entre la innovación y la protección de los derechos fundamentales.

2.1.2. La ley de Protección de Datos Personales: alcances y ámbito de aplicación

El ámbito de aplicación de la ley se limita estrictamente a la protección de los datos personales de las personas naturales, ya que son ellas quienes, por su condición, pueden ver comprometidos sus derechos fundamentales, como a la intimidad (personal y familiar), la privacidad y la autodeterminación informativa. Esta protección responde a la necesidad de evitar el uso indebido de su información en un contexto donde el acceso y tratamiento de datos pueden generar riesgos significativos para su dignidad y seguridad[10].

2.1.2.1. Alcances de la Ley de Protección de Datos Personales

2.1.2.1.1. Datos personales

Entendemos como datos personales a toda información que permite poder identificar a una persona natural mediante medios que, de manera razonable, puedan ser utilizados para dicho fin, conforme lo establece el artículo 2, inciso 4, de la Ley de Protección de Datos Personales.

---

[10] Defensoría del Pueblo, *Manual de Protección de Datos Personales* (Lima: Defensoría del Pueblo, 2019), https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf.

Además, un dato adquiere carácter personal cuando puede ser vinculado con una persona natural, incluso si quien lo posee no tiene la capacidad directa de establecer dicha relación, es decir que sin bien no lo identifica si lo puede hacer identificable[11]. Por ejemplo, una cuenta bancaria, por sí sola, no permite identificar a su titular; sin embargo, el banco sí puede asociarla con su identidad. Es por esta razón que sigue considerándose un dato personal, aun cuando quien la posea no pueda identificar directamente a la persona.

Cuando mencionamos que esta información puede ser obtenida de manera razonable, hacemos referencia a aquellos datos obtenidos con facilidad, ya que su acceso no requiere esfuerzos significativos para la persona que los solicita. Esto ocurre, por ejemplo, con la información contenida en el DNI, la foto montada en un fotochek, la voz del individuo, la firma realizada en un contrato o incluso una dirección de correo electrónico asociada a una cuenta personal.

Sin embargo, el hecho de que estos datos sean accesibles no significa que puedan ser utilizados libremente. Ahí es donde la protección de los datos personales, también conocida como autodeterminación informativa, juega un papel fundamental[12]. El derecho a la autodeterminación informativa tiene como finalidad asegurar que cada persona pueda proteger su vida privada ante posibles abusos o riesgos derivados del uso de su información personal[13].

Es importante considerar que la recopilación y el tratamiento de estos datos deben realizarse con el consentimiento del titular y en estricto respeto al propósito específico para el cual fueron solicitados, en concordancia con el marco normativo de protección de datos personales.

---

[11] Alvarado, *"La gestión de la seguridad de la información en el Régimen Peruano de Protección de Datos Personales"*, 28.
[12] Praeli, "*El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú"*, 132 -134.
[13] Defensoría del Pueblo, *Manual de Protección de Datos Personales* (Lima: Defensoría del Pueblo, 2019)

2.1.2.1.2. Datos sensibles

Mientras que los datos personales permiten la identificación de una persona, los datos sensibles están estrechamente relacionados con su esfera íntima, lo que les otorga un nivel de protección especial. Desde una perspectiva material, estos datos reflejan aspectos que definen la dignidad, personalidad y forma de ser del individuo. Desde un enfoque formal, su tratamiento exige garantías especiales que aseguren el respeto a la voluntad del titular[14].

Según el artículo 2, inciso 5, de la LPDP, se consideran datos sensibles aquellos que permiten identificar al titular y cuya divulgación podría generar discriminación o situarlo en una posición de desventaja dentro de un contexto social. Entre ellos se incluyen los datos biométricos que hacen identificables a las personas, así como información sobre su salud, vida sexual, origen racial, creencias y aspectos vinculados a su trabajo[15].

Un claro ejemplo de datos sensibles lo constituyen las historias clínicas y los exámenes de laboratorio, pues contienen información detallada y confidencial sobre la salud del paciente. Su divulgación sin autorización no sólo vulneraría su derecho a la intimidad, sino que también podría comprometer su integridad y generar consecuencias adversas en distintos ámbitos personales[16].

Debido a su naturaleza privada y al impacto que podría derivarse de un uso indebido, el tratamiento de los datos sensibles sólo es viable con el consentimiento expreso y por escrito del titular. No obstante, conforme al inciso 13.6 de la LPDP, su tratamiento será admisible cuando cuente con respaldo legal y responda a razones de interés público.

---

[14] Nataly Macutela Lavilla, "Tratamiento de datos personales sensibles en Perú en el contexto de Covid-19". (Tesis para optar el título de segunda especialidad en Derecho Administrativo, Pontificia Universidad Católica del Perú,2020),6.

[15] Zuleymi Velasco Pérez, "Derecho penal y protección de datos personales", *Llapanchikpaq:Justicia 6,* no.9 (2024): 137. https://revistas.pj.gob.pe/revista/index.php/lj/article/view/1042/1449

[16] Laisha Mubarak Aguad, "El internet, el Bigdata y el tratamiento de datos personales". *Advocatus*, no.36 (2017): 209.

2.1.2.1.3. Tratamiento de datos personales

La LPDP, en su artículo 2 inciso 19, define el tratamiento de datos como cualquier procedimiento, automatizado o no, que implique la recopilación, almacenamiento, uso, transferencia o supresión de información personal. Como regla general, el tratamiento de datos personales exige el consentimiento previo, informado, expreso e inequívoco del titular, ya que su uso sin autorización previa constituye una práctica ilegal. Dicho consentimiento puede otorgarse de forma verbal o escrita; sin embargo, en el caso de datos sensibles, es obligatorio que sea por escrito ya que se debe garantizar que el titular de los datos personales tenga pleno conocimiento de la entidad o persona a la que proporciona su información[17].

No obstante, el artículo 14 de la LPDP establece excepciones en las que no se requiere la autorización del titular, como cuando los datos son recopilados por entidades públicas en el ejercicio de sus funciones, instituciones financieras, centros médicos, empleadores en el ámbito laboral o en la ejecución de un contrato. En estos casos, dichas entidades solo pueden recolectar los datos estrictamente necesarios para el cumplimiento de sus fines. Por ejemplo, para solicitar un crédito hipotecario, no sería legítimo exigir información sobre la orientación sexual o religión del solicitante, ya que estos datos no guardan relación con la evaluación del crédito[18].

Cabe aclarar que, la exoneración del consentimiento no significa que se prescinda de las demás obligaciones y principios de protección de datos, como la finalidad específica del tratamiento y la adopción de medidas de seguridad adecuadas para garantizar la confidencialidad e integridad de la información.

---

[17] Raúl Vásquez Rodríguez, "El consentimiento para tratamiento de datos personales de salud en tiempos del COVID-19", *YachaQ Revista De Derecho*, no. 11 (2020): 154-155. https://doi.org/10.51343/yq.vi11.366.

[18] Defensoría del Pueblo, *Manual de Protección de Datos Personales* (Lima: Defensoría del Pueblo, 2019), https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf.

2.1.2.1.4. Banco de datos

Según lo que indica el artículo 2 inciso 1 de la LPDP, el banco de datos personales es un sistema organizado que almacena información de carácter personal en distintos formatos, ya sean físicos o digitales. Según su titularidad, pueden ser públicos o privados y gestionados de forma manual o automatizada.

En su funcionamiento intervienen tres actores clave: el titular de los datos personales, que es la persona natural a quien pertenece la información; el titular del banco de datos, ya sea una persona natural, jurídica o entidad pública, quien determina su finalidad, contenido y las medidas de seguridad aplicables; y el encargado del tratamiento, quien gestiona los datos por cuenta del titular del banco, dentro de los límites de una relación jurídica[19].

Esta estructura de actores es fundamental para garantizar una gestión adecuada de los datos personales, asegurando que su tratamiento se realice conforme a la normativa vigente y respetando los derechos de los titulares. En este sentido, la LPDP reconoce los derechos ARCO, como derechos que permiten a los titulares exigir un manejo adecuado de sus datos, brindándoles herramientas para su protección frente al responsable del banco de datos. En ese sentido, los derechos ARCO comprenden[20]:

- Derecho de acceso: Permite al titular conocer qué datos han sido recopilados, en qué entidad se encuentran almacenados y con qué finalidad fueron tratados o utilizados.

- Derecho de rectificación: Otorga la facultad de corregir o actualizar su información.

---

[19] Moore, *"Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales"*,438.

[20] Autoridad Nacional de Protección de Datos Personales, "Conoce tus derechos ARCO", Gob.pe, 16 de junio de 2022, https://cdn.www.gob.pe/uploads/document/file/5026755/CARTILLA%20ARCO%202022.pdf?v=1692715059

- Derecho de cancelación: Permite al titular solicitar la eliminación de sus datos cuando estos han dejado de cumplir la finalidad para la que fueron recopilados.

- Derecho de oposición: Faculta al titular a rechazar el tratamiento de sus datos en determinados supuestos.

Para garantizar la publicidad y transparencia sobre la existencia y características de los bancos de datos personales, la LPDP, en su artículo 34, establece la creación del Registro Nacional de Protección de Datos Personales, administrado por la Autoridad Nacional de Protección de Datos Personales (en adelante, la ANPD). En este sentido, todo banco de datos debe inscribirse en dicho registro con el propósito de salvaguardar los derechos del titular de la información y asegurar el cumplimiento de las disposiciones legales en materia de protección de datos[21].

Sin embargo, la autoridad supervisora sólo podrá acceder a su contenido en el marco de un procedimiento administrativo debidamente justificado. Asimismo, tanto el titular del banco de datos como el encargado de su tratamiento tienen la obligación de garantizar que el procesamiento de la información se realice con transparencia y legalidad. Todo ello con el objetivo de asegurar que la información personal se gestione conforme a los derechos ARCO y los principios de protección de datos personales.

2.1.2.1.5. Principios de la Ley de Protección de Datos Personales

La LPDP establece una serie de principios fundamentales que deben ser acatados por los titulares y responsables de los bancos de datos en el proceso de registro y tratamiento de la información personal de los ciudadanos. Entre estos principios se encuentran[22]:

---

[21] Praeli, *"El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú",*136-137.

[22] Moore,*"Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales"*,440-441.

- Principio de legalidad: La recopilación de datos personales debe realizarse conforme a la normativa vigente, prohibiéndose el uso de métodos fraudulentos, desleales o ilícitos.

- Principio de consentimiento: El tratamiento de los datos requiere la autorización expresa del titular.

- Principio de finalidad: Los datos deben ser recolectados con un propósito específico, legítimo y claramente determinado.

- Principio de proporcionalidad: La información recopilada debe ser adecuada, pertinente y no excesiva en relación con la finalidad para la cual es tratada.

- Principio de calidad: Los datos personales deben ser veraces, exactos y, en la medida de lo posible, mantenerse actualizados, asegurando su pertinencia y adecuación a la finalidad establecida.

- Principio de seguridad: Es obligatorio implementar medidas técnicas, organizativas y legales que garanticen la protección y resguardo de la información.

- Principio de disposición de recurso: Se debe garantizar a los titulares de los datos el acceso a mecanismos administrativos o judiciales que les permitan ejercer y hacer valer sus derechos.

- Principio de nivel de protección adecuado: En el caso de transferencia internacional de datos personales, se debe asegurar un nivel de protección suficiente para resguardar la información.

Para finalizar, los principios rectores de la LPDP constituyen el marco fundamental para garantizar un tratamiento adecuado de los datos personales, equilibrando el derecho a la privacidad con las necesidades legítimas de uso de la información.

2.1.2.2. Ámbito de aplicación de la Ley

La LPDP tiene como objetivo regular los procedimientos de almacenamiento, archivo, registro, sistematización y transmisión de datos personales gestionados por entidades públicas y privadas. Su finalidad es garantizar la protección del derecho fundamental reconocido en el artículo 2, inciso 6, de la Constitución Política del Perú, el cual prohíbe la divulgación de información que afecte la intimidad personal y familiar de los ciudadanos. En este contexto, la LPDP se configura como una norma de desarrollo constitucional, al establecer disposiciones que concretan y fortalecen la tutela de dicho derecho[23].

El artículo 3 de la LPDP delimita su ámbito de aplicación, estableciendo que sus disposiciones se extienden a los datos personales registrados o destinados a ser incorporados en bancos de datos gestionados por entidades públicas o privadas dentro del territorio nacional. Asimismo, la normativa contempla una protección reforzada para los denominados "datos sensibles", en virtud de su naturaleza y del potencial impacto que su tratamiento podría generar sobre los derechos de los titulares.

En respuesta a los constantes avances tecnológicos y los nuevos desafíos en materia de privacidad, se ha considerado necesario actualizar la regulación vigente para fortalecer la protección de los datos personales. Esta actualización se materializa con la reciente modificación del Reglamento de la LPDP, que introduce cambios significativos orientados a reforzar las medidas de seguridad y garantizar los derechos de los titulares.

El Reglamento de la LPDP fue actualizado mediante el Decreto Supremo 016-2024-JUS, publicado el 30 de noviembre de 2024. Esta nueva versión incorpora modificaciones significativas y refuerza la protección de los datos personales en diversos ámbitos. Entre las principales novedades del reglamento se encuentran[24]:

---

[23] Praeli, *"El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú",*134.

[24] Elani Yahaira Mamani Gutiérrez, "Reglamento de la ley de protección de datos personales [Decreto Supremo 016-2024-JUS], Lp Pasión por el Derecho, 30 de noviembre de 2024, https://lpderecho.pe/reglamento-ley-proteccion-datos-personales-decreto-supremo-016-2024-jus/

- Notificación obligatoria de incidentes de seguridad: Las organizaciones deberán informar a la ANPD sobre cualquier incidente de seguridad en un plazo máximo de 48 horas.
- Derecho a la portabilidad de datos personales: Se reconoce expresamente el derecho de los ciudadanos a trasladar sus datos de un proveedor a otro de manera estructurada y en un formato adecuado.
- Fortalecimiento de las medidas de seguridad: Se exige la implementación de políticas de seguridad con fecha cierta, asegurando una protección más robusta de la información.
- Regulación del uso de datos personales en publicidad y prospección comercial: Se establecen lineamientos específicos para el tratamiento de la información en campañas publicitarias.
- Nueva clasificación de infracciones: Se redefinen las infracciones en leves, graves y muy graves, estableciendo sanciones diferenciadas.
- Evaluaciones de impacto en privacidad (PIA): Se requiere la realización de estudios previos sobre los riesgos en la privacidad antes de implementar tratamientos de datos personales.
- Regulación de procesos automatizados: Se establecen reglas para decisiones basadas únicamente en procesos automatizados sin intervención humana.
- Representación de titulares extranjeros: Se exige la designación de un representante legal en Perú para los titulares de bancos de datos personales ubicados fuera del país.

Estas disposiciones fortalecen el marco normativo de protección de datos personales, garantizando mayor control y seguridad para los ciudadanos. Además, el decreto establece con mayor precisión las sanciones en caso de incumplimiento, contemplando multas administrativas considerables, y fortaleciendo las atribuciones de la ANPD para supervisar y asegurar el cumplimiento de la normativa.

2.2. Derechos fundamentales involucrados en la protección de datos personales

2.2.1. Derecho a la privacidad

2.2.1.1. Origen del derecho a la privacidad

Las primeras referencias expresas a la intimidad o a la vida privada, como un derecho autónomo, surgen en los Estados Unidos a finales del siglo XIX, en torno al concepto de *right of privacy*. Destaca en este contexto la contribución del juez Thomas Cooley en *The Elements of Torts* de 1879, donde define este derecho como "el derecho a ser dejado solo", libre de perturbaciones externas no deseadas. Un momento crucial en su desarrollo lo constituyó el artículo *The Right of Privacy*, publicado en *Harvard Law Review* el 15 de diciembre de 1890 por Samuel Warren y Louis Brandeis[25].

Warren, al estar casado con la hija de un senador, le preocupaba e incomodaba la divulgación de aspectos de su vida conyugal debido al intenso escrutinio de la prensa sensacionalista. Es por ello que subrayó en su artículo la importancia del derecho de toda persona a vivir en paz, proteger su privacidad y resguardar su vida íntima[26]. En este contexto, el *Common Law* reconoce a cada individuo la facultad de decidir en qué medida desea compartir sus pensamientos, sentimientos y emociones, garantizando así su tranquilidad espiritual y bienestar personal. Esta concepción se aparta de la tradicional protección de la propiedad privada que predominaba en la época, estableciendo la privacidad como un derecho inherente a la inviolabilidad de la persona[27].

Desde esta perspectiva, el derecho a la privacidad se configura como la facultad de rechazar cualquier intromisión no consentida en la esfera personal, con especial énfasis en la protección frente a la injerencia de los medios de comunicación en aspectos sensibles como la vida doméstica y las relaciones interpersonales.

---

[25] Praeli, *"La libertad de información y su relación con los derechos a la intimidad y al honor en el caso Peruano*", 53.
[26] Jonathan López Torres, "Antecedentes internacionales en materia de privacidad y protección de datos personales", 104-105.
[27] Mónica Jara Villacís, "El derecho a la intimidad y la presentación de correos electrónicos como prueba". (Tesis para optar el grado de Especialista en Derecho Constitucional, 2013), 10.

No obstante, a pesar de las aportaciones conceptuales sobre privacidad e intimidad, estas no tuvieron un impacto inmediato en las decisiones de los tribunales. Sin embargo, la situación cambiaría en los años siguientes cuando las cortes empezaron a recibir con mayor frecuencia casos en donde las personas alegaban haber sido perjudicadas por la difusión de una publicación o fotografía sin su consentimiento.

Un ejemplo de ello ocurrió en 1902, cuando la Corte de Apelaciones de Nueva York resolvió, en el caso *Roberson vs. Rochester Folding Box Co*., que el derecho a la privacidad no tenía reconocimiento legal, dejando a la víctima sin protección ante el uso no autorizado de su imagen. Este fallo generó gran controversia y llevó a la legislatura de Nueva York a aprobar una norma que prohibía el uso comercial de retratos sin consentimiento. Sin embargo, en 1905, la Corte Suprema de Georgia, en el caso *Pavensich vs. New England Life Insurance Co*., se apartó de este criterio y reconoció expresamente la existencia del *right to privacy,* estableciendo así un precedente jurisprudencial que marcaría el desarrollo posterior de este derecho[28].

Años más tarde, en 1967, el profesor Alan Furman Westin realizó un importante aporte teórico sobre el concepto de privacidad. En su obra, definió la privacidad como el derecho de cada persona a "controlar, editar, gestionar y eliminar la información sobre sí mismo, así como decidir cuándo, cómo y en qué medida dicha información es compartida con los demás", una noción que más adelante sería adoptada expresamente por el Tribunal Constitucional Federal Alemán en su sentencia del 15 de diciembre de 1983 sobre el Censo de 1933[29].

El derecho a la privacidad ha evolucionado significativamente a lo largo del siglo XX, consolidándose como un derecho fundamental en distintos instrumentos jurídicos internacionales y nacionales. Aunque la protección de la esfera íntima tiene antecedentes históricos, su configuración jurídica moderna es relativamente reciente.

---

[28] Milagros Katherine Olivos Celis, "La protección de la privacidad como objeto de tutela en el ordenamiento jurídico Peruano", *IUS: Revista de Investigación de la Facultad de Derecho* 8, no.1 (2019): 50-51. https://doi.org/10.35383/ius.v1i1.38.

[29] Olivos, *"La protección de la privacidad como objeto de tutela en el ordenamiento jurídico Peruano"*, 51

Un hito fundamental en este proceso es la Declaración Universal de Derechos Humanos de 1948, cuyo artículo 12 establece que toda persona tiene derecho a la protección de la ley contra injerencias arbitrarias o ataques que vulneren su honra, vida privada o familiar[30]. Este reconocimiento sentó las bases para que otros instrumentos internacionales adoptarán disposiciones similares. Por ejemplo, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, en su artículo 8.1 y el Pacto Internacional de Derechos Civiles y Políticos de 1966, en su artículo 17 que refuerzan la protección de esta esfera privada[31].

En América Latina, la Convención Americana sobre Derechos Humanos de 1969, en su artículo 11, también consagra el derecho a la privacidad, prohibiendo intervenciones arbitrarias que afecten la honra o la dignidad personal. Estas normativas reflejan una creciente preocupación global por resguardar la vida privada frente a posibles vulneraciones, tanto por parte del Estado como de actores privados.

En el ordenamiento jurídico peruano, el derecho a la privacidad no se menciona expresamente como una categoría autónoma, sino que sus distintas manifestaciones han sido desagregadas en derechos específicos, como la intimidad o la inviolabilidad de las comunicaciones. No obstante, la legislación que desarrolla este modelo de protección emplea la denominación "protección de datos personales" para referirse a la salvaguarda de la vida privada.

Así, el artículo 1 de la LPDP reconoce como su objeto de tutela la garantía del derecho fundamental previsto en el artículo 2.6 de la Constitución, el cual protege a las personas frente a la exposición de su información personal o familiar, o a que terceros la divulguen sin su consentimiento, ya sea a través de servicios informáticos o por otros medios. De este modo, la norma identifica expresamente la privacidad como su ámbito de protección[32].

---

[30] Organización de las Naciones Unidas, "Declaración Universal de Derechos Humanos", Naciones Unidas, 10 de diciembre de 1948. https://www.un.org/es/about-us/universal-declaration-of-human-rights.

[31] María Solange Maqueo Ramírez., Jimena Moreno Gonzáles, Miguel Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario." *Revista de Derecho XXX*, no. 1 (2017):80-81, https://www.redalyc.org/articulo.oa?id=173752279004

[32] Olivos, *"La protección de la privacidad como objeto de tutela en el ordenamiento jurídico Peruano"*, 59

2.2.1.2. Protección de la privacidad en entornos digitales

Cuando se habla de privacidad, se hace referencia a un ámbito de la vida personal que está resguardado de la intervención del Estado y del escrutinio de terceros, ya que concierne exclusivamente a la esfera individual de cada persona. Por esta razón, tradicionalmente se ha vinculado con el derecho a estar solo. Sin embargo, en la actualidad, el concepto abarca múltiples dimensiones, como las libertades individuales, la inviolabilidad del domicilio, la confidencialidad de las comunicaciones, la facultad de controlar los datos personales, la autodeterminación sobre el propio cuerpo y la protección frente a la vigilancia no justificada[33].

Esta transformación responde a la creciente interconexión digital, donde la exposición de la información personal se ha convertido en un desafío constante. La evolución del concepto de privacidad ha estado marcada por el impacto de los medios de comunicación y la tecnología, desde el auge del periodismo de investigación y la televisión sensacionalista, que pusieron en debate los límites de la privacidad, hasta la era digital, en la que la inteligencia artificial y la recopilación masiva de datos han redefinido la protección de la información personal[34].

Un ejemplo reciente de esta vulnerabilidad es el caso de Interbank, que el 30 de octubre de 2024 confirmó la exposición no autorizada de datos de un grupo de clientes debido a un ataque cibernético. La Fiscalía en Ciberdelincuencia de Lima Centro inició diligencias preliminares para investigar el presunto delito informático. Este hecho constituye una vulneración a la privacidad, al implicar el acceso no autorizado y la exposición de datos personales, evidenciando los riesgos del entorno digital[35]. En este contexto, la privacidad ya no solo implica un resguardo frente a injerencias externas, sino también una gestión activa de la propia identidad en entornos digitales.

---

[33] Peschard, "Cien años del derecho a la privacidad en la Constitución, 361-378", 363.

[34] Sentencia del Tribunal Constitucional. Exp.. N.º 6712-2005-HC/TC, 17 de octubre de 2005, derecho a la intimidad y la protección de la vida privada, reconociéndose como aspectos fundamentales de la dignidad humana.

[35] Gestión, "Interbank: Fiscalía en ciberdelincuencia inició diligencias sobre presunto hackeo", *Gestión,* 30 de octubre de 2024, *https://gestion.pe/economia/interbank-hackeo-fiscalia-en-ciberdelincuencia-inicio-diligencias-sobre-presunto-hackeo-indecopi-datos-de-usuarios-noticia/?utm_source=chatgpt.com*

2.2.2. Derecho a la intimidad

2.2.2.1. Origen del derecho a la intimidad

El derecho a la vida íntima y privada surgió como respuesta a la expansión del poder político, estableciendo límites a su intervención en la esfera personal de los individuos. Su origen está estrechamente vinculado a la afirmación de la libertad frente al Estado, configurándose como un conjunto de facultades que garantizan la exclusión de cualquier injerencia en los aspectos más reservados de la vida privada[36].

Aunque su reconocimiento expreso en las constituciones y pactos internacionales de derechos humanos es relativamente reciente, sus raíces se remontan al surgimiento mismo de la noción de libertad personal y a la necesidad de preservar ámbitos de autodeterminación libres de intrusión, injerencia externa o divulgación, especialmente por parte del poder público.

El desarrollo de la concepción moderna de la intimidad se vio influenciado por factores como la alfabetización y la búsqueda de la soledad, que fortalecieron el individualismo y consolidaron este derecho como esencial. Doctrinalmente, esta idea se apoyó en el pensamiento de Thomasius y Kant, quienes defendían la existencia de un ámbito interno ajeno al control estatal[37].

Sin embargo, no puede desvincularse su evolución de las aportaciones filosóficas del Liberalismo, especialmente de autores anglosajones como Locke, Price y John Stuart Mill, quienes promovieron la libertad y autonomía personal como pilares fundamentales de un régimen político opuesto al poder absoluto del gobernante. En ese sentido, estos autores no sólo defendieron la libertad frente a la autoridad, sino que también destacaron la importancia de un espacio personal inviolable, clave para el desarrollo moral y político del individuo[38].

---

[36] Ana Garcia Domínguez, *Tratamiento de Datos Personales y Derechos Fundamentales* (Madrid: Editorial DYKINSON,2024), 19.

[37] Jorge Eugenio Dotti, "Observaciones sobre Kant y el Liberalismo", *Araucaria* 7, no.13 (2005): 5. https://revistascientificas.us.es/index.php/araucaria/article/view/1088.

[38] Dalmacio Negro Pavón, "John Stuart Mill: el liberalismo como ideología", *Revista de estudios políticos* 159, no.1 (1968): 126.

El derecho a la intimidad comenzó a reconocerse como un derecho autónomo en Estados Unidos a finales del siglo XIX, con aportes clave como los del juez Thomas Cooley o los aportes de Samuel Warren y Louis Brandeis. En el caso peruano, el *right of privacy* ha influido en la construcción del derecho a la privacidad y a la intimidad, consolidándose como una garantía fundamental para proteger la esfera personal frente a injerencias indebidas[39].

Si bien su reconocimiento jurídico es reciente, el derecho a la intimidad se considera parte de los derechos de primera generación, vinculados a la dignidad y autonomía del individuo en el marco del Estado liberal. Así, ha pasado de ser una noción abstracta a convertirse en un componente esencial de la protección de los derechos humanos en las sociedades actuales.

Por su parte, el Perú, aunque sigue el modelo del *Civil Law*, también reconoce la intimidad como un derecho fundamental. La Constitución, en su artículo 2, inciso 7, consagra el derecho de toda persona a la intimidad personal y familiar. Esta protección se refuerza a través del Código Civil, por medio de su artículo 14 el cual indica que la intimidad de un individuo o de su familia no puede ser divulgada sin su consentimiento; y la LPDP, la cual establece mecanismos para la protección del derecho a la intimidad de los individuos, limitando la intromisión de terceros y regulando el acceso a la información personal[40].

A diferencia del *Common Law*, donde la protección de la vida íntima y privada se desarrolla a través de precedentes judiciales, en el sistema peruano este derecho se encuentra definido y regulado mediante disposiciones normativas expresas que delimitan su alcance y garantías.

El derecho a la intimidad salvaguarda la información sensible que revela aspectos esenciales de la identidad personal, accesible únicamente al individuo o a quienes éste decida compartir su información.[41]

---

[39] Praeli, *"La libertad de información y su relación con los derechos a la intimidad y al honor en el caso Peruano*", 53.

[40] Juan Morales Godo, "Derecho al honor, buena reputación, intimidad personal y familiar, voz e imagen", en *La Constitución comentada* (Lima: Gaceta jurídica, 2005), 275-277.

[41] Marcos Alejandro Celis Quintal, "La protección de la intimidad como derecho fundamental de los Mexicanos, en *Protección de la persona y derechos fundamentales* (México: UNAM, 2006),74.

En este sentido, el derecho a la intimidad se configura como un espacio de libertad esencial para el desarrollo pleno del individuo. Su reconocimiento ha sido el resultado de un proceso histórico en el que se ha consolidado como un límite frente a las injerencias del poder y como una garantía esencial para la autodeterminación personal, siendo este un derecho irrenunciable.

2.2.2.2. Protección de la intimidad en entornos digitales

El desarrollo de la informática ha hecho más fácil recopilar, organizar y analizar los datos que las personas generan a lo largo de su vida. Esto permite que terceros creen perfiles de comportamiento basados en esa información. Sin embargo, esta capacidad de observar y predecir las acciones de las personas puede limitar su libertad individual, lo que ha llevado a revalorar el derecho a la intimidad.

El derecho a la intimidad no se limita al derecho de excluir a otros del ámbito privado, sino que implica un espacio de resguardo inviolable que protege la identidad única de cada persona. Sin embargo, en el entorno digital actual, esta protección se encuentra amenazada. Las grandes plataformas digitales y redes sociales han transformado la manera en que se accede a la información personal, haciendo que los datos más sensibles de los usuarios, incluidos los biométricos, sean recopilados y procesados bajo el pretexto de reforzar la seguridad o adaptar los servicios a las preferencias del usuario[42].

Uno de los principales problemas que podemos identificar es la aparente voluntariedad del consentimiento otorgado por los usuarios. Si bien estos aceptan los términos y condiciones antes de utilizar un servicio, en la práctica, esta aceptación no es una decisión libre, sino una condición impuesta para acceder a herramientas esenciales en la vida digital. Este modelo obliga a las personas a ceder parte de su intimidad a cambio de participación en el mundo digital, sin garantías suficientes sobre el manejo de su información más sensible[43].

---

[42] María Belén Chilano, "Intimidad en la era digital: análisis jurídico y enfoque juvenil sobre percepciones y prácticas", *Derecom. Derecho de la Comunicación y de las Nuevas Tecnologías*, no.35 (2024): 42. https://revistas.ucm.es/index.php/DERE/article/view/98693

[43] Gerard Henry Angles Yanqui, "TikTok:La ineficacia del derecho a la intimidad en la era digital en tiempos de Covid-19 y el "famoso" derecho al olvido en Perú", *Revista de Derecho* 5, no.1 (2020): 198.

A pesar de la existencia de normativas orientadas a la protección de datos personales, la asimetría de poder entre los usuarios y las plataformas digitales continúa en aumento, especialmente con la recopilación de sus datos biométricos. La naturaleza irrepetible de estos datos los hace particularmente vulnerables a accesos indebidos y usos no autorizados, pues, a diferencia de una contraseña, no pueden ser modificados en caso de filtración. Esta situación se agrava con la interacción constante en redes sociales, que transforma la percepción y resguardo de la privacidad. Ante estos riesgos, resulta fundamental contar con mecanismos jurídicos, como el habeas data, que permitan salvaguardar la privacidad y la autodeterminación informativa en el entorno digital.[44].

Frente a este escenario, resulta necesario reforzar los mecanismos de resguardo del derecho a la intimidad en el ámbito digital. La regulación debe garantizar que la recopilación de información altamente sensible se realice bajo estrictos estándares de seguridad y con un consentimiento verdaderamente informado.

2.2.3. Diferencia entre privacidad e intimidad

La noción de "intimidad" constituye un concepto esencial que ha generado múltiples debates en torno a su significado, ocupando un lugar central en las discusiones éticas, políticas, sociales y jurídicas. No existía un término único que delimite con precisión ese espacio personal de libertad que se pretende proteger frente a intervenciones indeseadas[45].

Es por ello que el término "privacidad", derivado del anglicismo *privacy*, en sus inicios tenía un uso más amplio para referirse a la vida privada en general, antes de que su significado se diferenciara con mayor precisión del concepto de "intimidad" en los sistemas jurídicos de tradición continental (Civil Law).

---

[44] Juan Morales Godo, "El derecho a la intimidad y el conflicto con el derecho a la información", en *La Constitución comentada* (Lima: Gaceta jurídica, 2005), 119-120.

[45] José María Martínez de Pisón Cavero, "El Derecho a la Intimidad : De la configuración inicial a los últimos desarrollos de la jurisprudencia constitucional", *Anuario de filosofía del Derecho*, no.32 (2016): 412-413, https://revistas.mjusticia.gob.es/index.php/AFD/article/view/2301.

Dentro de la construcción doctrinal y jurisprudencial del derecho a la intimidad, la tradición alemana ha buscado delimitar su contenido mediante la denominada "teoría de las esferas" (*Sphärentheorie*), desarrollada inicialmente por el jurista Heinrich Hubmann. Esta teoría surgió con el propósito de diferenciar el ámbito privado del ámbito público en la protección de la intimidad. A lo largo del tiempo, su desarrollo doctrinal y jurisprudencial ha permitido una comprensión más matizada de sus límites jurídicos[46].

Según la concepción estructural de las esferas concéntricas, resulta complejo delimitar con precisión los conceptos de intimidad y privacidad, ya que no se consideran nociones completamente separadas, sino elementos interrelacionados dentro de un mismo sistema. Bajo esta perspectiva, la privacidad abarca una esfera amplia que comprende distintos aspectos de la vida personal, mientras que la intimidad constituye el núcleo más restringido y protegido, reflejando los aspectos más profundos del ser humano, su mundo interno o incluso su dimensión espiritual[47].

Desde el punto de vista de los derechos fundamentales, esta distinción resulta importante porque la esfera más íntima requiere no solo reconocimiento legal, sino también mecanismos efectivos de protección contra cualquier vulneración que pueda afectarla.

Un ejemplo ilustrativo de esta diferenciación es el caso *Griswold vs. Connecticut* (1965), en el que el Tribunal Supremo de los Estados Unidos declaró inconstitucional la prohibición de vender, distribuir y utilizar anticonceptivos, al considerar que dicha restricción vulneraba la esfera más íntima de las personas. La Corte no solo reconoció la privacidad en términos generales, sino que destacó que la intimidad implica el derecho a tomar decisiones trascendentales sobre la propia vida sin injerencias externas. Este fallo evidenció que la intimidad no se limita a la protección frente a la divulgación de información personal, sino que también resguarda la autodeterminación en asuntos profundamente personales, como la planificación familiar[48].

---

[46] Andoni Polo Roca, "Privacidad, intimidad y protección de datos: Una mirada Estadounidense y europea", *Derechos y libertades: Revista de Filosofía del Derecho y Derechos Humanos*, no.47 (2022): 316 -319, https://doi.org/10.20318/dyl.2022.6884.

[47] Jaccottet, *"Privacidad, intimidad: Un debate sobre los alcances de las limitaciones a los Derechos Fundamentales y la visión de la libertad de expresión ante la novela 1984 de George Orwell"*,84.

[48] Praeli, *"La libertad de información y su relación con los derechos a la intimidad y al honor en el caso Peruano"*, 53.

Lo que el fallo refuerza es la idea de que la intimidad no solo implica el resguardo frente a la divulgación de información personal (lo que suele asociarse con la privacidad), sino que también abarca la autonomía para tomar decisiones fundamentales sobre la vida personal.

Desde la teoría de las esferas concéntricas, se puede entender que privacidad e intimidad están interrelacionadas, pero la intimidad exige un nivel de protección mucho más elevado. En este sentido, el fallo de la Corte Suprema en *Griswold* resalta la importancia de proteger no solo la información personal, sino también la capacidad de los individuos para ejercer su autodeterminación en asuntos íntimos.

La teoría de las esferas, originada en la doctrina alemana, ha constituido un referente esencial para delimitar los conceptos de intimidad y privacidad en la protección de los derechos fundamentales en el Perú. Esta teoría estructura la vida personal en distintos niveles, otorgando una tutela más estricta a las áreas de mayor reserva.

En la jurisprudencia peruana, el Tribunal Constitucional ha recogido esta distinción, en la Sentencia 166/2021, donde se estableció que la vida privada abarca aspectos personales accesibles a un círculo más amplio, mientras que la intimidad se refiere a la esfera más reservada del individuo[49]. Como se expuso en apartados previos, la divulgación no consentida de esta última puede derivar en afectaciones significativas, lo que justifica una tutela jurídica más estricta.

2.2.4. El derecho al acceso informativo

2.2.4.1 Definición y marco normativo

El derecho de acceso a la información es una garantía fundamental que permite a toda persona solicitar y obtener datos de entidades públicas sin necesidad de justificar su petición, conforme a lo establecido en el inciso 5 del artículo 2 de la Constitución. Esta facultad, protegida a través del hábeas data, asegura la transparencia y el control ciudadano sobre la gestión pública. No obstante, dicho derecho encuentra límites en la protección de la intimidad personal y en aquellas excepciones previstas por ley o por razones de seguridad nacional.

[49] Tribunal Constitucional del Perú. Sentencia N° 166/2021, de 2 de febrero de 2021, que aborda la distinción entre vida privada e intimidad en relación con los registros de asistencia biométrica de los empleados públicos.

En este sentido, la información pública se presume accesible, y cualquier restricción debe ser excepcional y debidamente justificada. La carga de la prueba recae exclusivamente en el Estado, quien debe demostrar que la reserva responde a un interés público apremiante y cumple con un objetivo constitucional legítimo. De lo contrario, la limitación al acceso a la información resultaría inconstitucional, vulnerando los principios de transparencia y control ciudadano[50].

Si bien el derecho de acceso a la información pública cuenta con un desarrollo normativo a nivel nacional, su fundamento se encuentra también en compromisos internacionales asumidos por el Estado. Instrumentos como la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos reconocen este derecho como parte esencial de la libertad de expresión y el acceso a la información.

En este contexto, la legislación peruana, a través de la Ley N.° 27806, Ley de Transparencia y Acceso a la Información Pública, desarrolla el ejercicio de este derecho al establecer los procedimientos específicos para requerir información a las entidades del Estado, conforme a lo señalado en su Reglamento, aprobado por el Decreto Supremo N.º 072-2003-PCM, y sus modificaciones introducidas por el Decreto Supremo N.º 070-2013-PCM. Su contenido refuerza la presunción de publicidad de la información pública y delimita los supuestos en los que su acceso puede restringirse, incluyendo aquellas excepciones expresamente señaladas en su Texto Único Ordenado (TUO). En este sentido, la información protegida bajo estas excepciones queda excluida del conocimiento público[51].

Asimismo, la LPDP complementa el marco normativo del derecho de acceso a la información pública al regular los límites en el tratamiento y divulgación de datos personales por parte de las entidades públicas.

---

[50] Sentencia del Tribunal Constitucional, EXP.N°2579-2003-HD/TC, 6 de abril de 2004, se refiere al derecho de acceso a la información pública y la autodeterminación informativa, destacando la transparencia en la administración y el control ciudadano.

[51] Defensoría del Pueblo, *Manual de excepciones al acceso a la información pública* (Lima: Defensoría del Pueblo, 2016), https://www.defensoria.gob.pe/wp-content/uploads/2018/08/Manual-excepciones-al-acceso-info-publica-2016.pdf.

2.2.4.2. El principio de publicidad en las entidades estatales

De acuerdo con la Ley de Transparencia, su artículo 2 establece que las entidades de la administración pública son aquellas definidas en el Artículo I del Título Preliminar de la Ley N° 27444 - Ley del Procedimiento Administrativo General. Entre estas entidades, el inciso 5 del mencionado artículo reconoce a los gobiernos locales como sujetos obligados a cumplir con las disposiciones de la Ley de Transparencia.

En virtud de su pertenencia a la Administración Pública, las municipalidades están sujetas a las obligaciones previstas en el Artículo 3 de la Ley N.° 27806, que consagra el principio de publicidad. Este principio establece que toda información que las entidades del Estado posean, produzcan, generen o procesen debe estar accesible para la ciudadanía, sin importar su formato. Esto incluye documentos escritos, grabaciones de audio o video, soportes digitales, fotografías, copias de contratos y montos acordados entre la municipalidad y empresas, así como información sobre presupuestos asignados a sectores específicos, como hospitales, y datos sobre la cantidad de especialistas que trabajan en ellos[52].

A pesar de lo establecido en el principio de publicidad, el acceso a cierta información puede verse restringido por razones de privacidad y seguridad. La Ley de Transparencia, en sus artículos 15 y 17, establece excepciones al derecho de acceso a la información pública, entre las cuales se encuentra aquella que comprometa la intimidad personal o familiar. En este sentido, si bien la normativa menciona que las grabaciones de audio y video generadas por entidades públicas forman parte de la información accesible, su entrega no es automática ni irrestricta. En el caso específico de las cámaras de videovigilancia administradas por las municipalidades, el acceso a sus grabaciones se encuentra limitado cuando su difusión podría afectar derechos fundamentales de terceros[53].

[52] Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP), *Saber es tu poder: Derecho al acceso a la información pública* (Lima: Ministerio de Justicia y Derechos Humanos, 2023), https://www.gob.pe/institucion/antaip/informes-publicaciones/3455744-saber-es-tu-poder-derecho-al-acceso-a-la-informacion-publica.

[53] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva 011-2023-JUS/DGTAIPD, de 21 de marzo de 2023, se refiere al acceso a imágenes, videos y audios captados por cámaras de videovigilancia en espacios públicos los cuales están limitados por la protección de datos personales.

2.3. Implementación de sistemas biométricos en el estado Peruano

2.3.1. Datos biométricos y sistemas biométricos

En la era digital, donde los datos son el recurso más valioso y la información fluye sin fronteras, la biometría se ha convertido en una pieza clave para la identificación de las personas. Basada en características físicas o rasgos biológicos únicos (huellas dactilares, estructura facial, el iris y los patrones de voz), esta tecnología se integra en un modelo que prioriza la recopilación y uso masivo de datos. En un mundo donde la información personal adquiere un valor comparable al de una moneda de cambio, garantizar su protección no es solo una necesidad, sino una urgencia[54].

Los sistemas biométricos han cobrado especial relevancia al permitir la captura y análisis de información altamente sensible mediante mediciones y estudios estadísticos de características biológicas. Mediante sistemas de captación de datos tales como los sensores de huellas, cámaras de reconocimiento facial, software de análisis de voz o el escáner de iris son datos únicos en cada individuo y, en muchos casos, imposibles de modificar. Su creciente implementación en sistemas automatizados de identificación y autenticación ha potenciado su importancia, especialmente en un mundo interconectado, donde la movilidad de personas y bienes genera tanto oportunidades como desafíos en materia de seguridad y privacidad[55].

Siguiendo esta misma línea, la biometría no solo se limita a la identificación individual, sino que también implica la gestión y almacenamiento de datos característicos de una persona o incluso de un grupo. Estos datos, administrados por entidades responsables, conforman perfiles biológicos utilizados principalmente para la verificación de identidad en ámbitos como la seguridad, el acceso a servicios y el control migratorio. Su creciente implementación en sistemas públicos y privados plantea desafíos en cuanto a su resguardo y uso, especialmente considerando los riesgos de exposición y mal uso de esta información altamente sensible[56].

---

[54] Silvia Barona Vilar, "Tecnologia biometrica y datos biométricos.Bondades y peligros. No todo vale", *Actualidad Jurídica Iberoamericana*, no. 21 (2024): 300-302, https://revista-aji.com/wp-content/uploads/2024/07/AJI21_Art11.pdf

[55] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 032-2021-JUS/DGTAIPD, de 17 de agosto de 2021, se refiere al uso de datos biométricos y su empleo en la identificación de personas, tratamiento de datos y gestión de derechos ARCO.

[56] Nathaly Macutela Lavilla, "Tratamiento de datos personales sensibles en Perú en el contexto de Covid-19". (Tesis de Segunda Especialidad en Derecho Administrativo, PUCP, 2020), 6-7.

2.3.2. Datos personales sensibles a través de sistemas biométricos

Como se mencionó anteriormente, los datos personales sensibles incluyen información que, por su naturaleza, requiere un tratamiento especial y una mayor protección jurídica para prevenir su uso indebido. Dentro de esta categoría se encuentran los datos biométricos, que permiten la identificación única de una persona a partir de características físicas, fisiológicas o conductuales.

Inicialmente, los sistemas biométricos dependían de sensores físicos instalados en espacios específicos, como edificios o salas, pero su evolución ha permitido su integración en dispositivos corporativos y sistemas informáticos. Hoy en día, la biometría combina distintos factores de autenticación, como características físicas y elementos de seguridad adicionales, optimizando la protección de la identidad en diversos contextos. Estos sistemas se utilizan en el control de asistencia laboral mediante reconocimiento de huellas, en la seguridad bancaria para validar transferencias, en centros de atención al cliente mediante reconocimiento de voz, en el control de acceso a redes y plataformas digitales, en la vigilancia policial a través de reconocimiento facial y análisis de patrones de movimiento, aunque con restricciones normativas[57].

No obstante, el tratamiento de datos biométricos a través de estas tecnologías plantea importantes desafíos en materia de privacidad y seguridad, ya que involucra información única y prácticamente irremplazable en caso de filtración o uso indebido. Por ello, la implementación de estos sistemas debe ajustarse a principios de legalidad, finalidad y proporcionalidad, garantizando que su uso no vulnere derechos fundamentales ni implique una recopilación masiva e indiscriminada de datos[58]. La creciente versatilidad de la biometría ha impulsado su adopción global, pero también ha intensificado el debate sobre la necesidad de un marco regulatorio que proteja adecuadamente la privacidad de las personas frente a los riesgos inherentes a estas tecnologías.

---

[57] Silvia Barona Vilar, "Tecnologia biometrica y datos biométricos.Bondades y peligros. No todo vale", *Actualidad Jurídica Iberoamericana*, no. 21 (2024): 304, https://revista-aji.com/wp-content/uploads/2024/07/AJI21_Art11.pdf

[58] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 032-2021-JUS/DGTAIPD, de 17 de agosto de 2021, se refiere al uso de datos biométricos y su empleo en la identificación de personas, tratamiento de datos y gestión de derechos ARCO.

En el Perú, el almacenamiento y administración de datos biométricos está principalmente a cargo del RENIEC, entidad responsable de la identificación oficial de los ciudadanos. Entre los sistemas de identificación biométrica implementados por el Registro Nacional de Identificación y Estado Civil (en adelante RENIEC) se encuentran el Sistema Automatizado de Identificación de Huellas Dactilares (en adelante AFIS) y el reconocimiento facial, entre otros. Cabe destacar que el RENIEC es la única entidad encargada de organizar y mantener el registro único de identificación de personas naturales, incluyendo sus datos biométricos, a través de los registros dactiloscópico y pelmatoscópico[59].

No obstante, diversas empresas pueden utilizar esta información para verificar la identidad de sus clientes o autenticar la información de una persona en específico, pero no necesariamente la almacenan de manera permanente, ya que en algunos casos solo la contrastan con la base de datos del RENIEC. Sin embargo, otras crean sus propias bases de datos biométricas para gestionar la identificación de manera autónoma. Toda entidad que procese o almacene datos biométricos debe cumplir con la LPDP y las disposiciones de la ANPD, garantizando un tratamiento seguro y respetando los derechos de los titulares, considerando que se trata de información altamente sensible e irremplazable en caso de vulneración.

Un ejemplo concreto de esta interacción regulada se refleja en la supervisión ejercida por la Superintendencia de Banca, Seguros y AFP (SBS), la cual, a través del Reglamento para la Gestión de la Seguridad de la Información y Ciberseguridad, exige a las entidades supervisadas la implementación de un mecanismo de doble factor de autenticación para aquellas operaciones que puedan implicar un riesgo o perjuicio para el usuario. Entre las opciones disponibles, este mecanismo puede incluir la autenticación biométrica. En este contexto, el RENIEC, al gestionar información biométrica en su base de datos, permite a las entidades bancarias validar la identidad de sus usuarios con mayor precisión, complementando así los procesos de autenticación con datos asociados a la identificación personal[60].

---

[59] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 032-2021-JUS/DGTAIPD, de 17 de agosto de 2021, se refiere al uso de datos biométricos y su empleo en la identificación de personas, tratamiento de datos y gestión de derechos ARCO.

[60] Boletín semanal SBS, “Servicios Financieros digitales: el uso de la biometría para proteger las operaciones financieras”, Superintendencia de Banca, Seguros y AFP (SBS), 6 de marzo de 2025, https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/2293

Si bien las entidades privadas utilizan información biométrica con la finalidad de identificar y proteger a los ciudadanos, resulta pertinente analizar si las medidas empleadas en todos los casos son proporcionales a la acción que realizan. En ese sentido, el principio de proporcionalidad, reconocido en la LPDP, exige que el tratamiento de datos personales sean necesarios,adecuados y no excesivos en relación con la finalidad perseguida. Sin embargo, en el contexto peruano, ha habido casos en los que este principio no ha sido respetado, como lo demuestra la reciente sanción impuesta al Banco de Crédito del Perú (en adelante BCP) por la ANPD[61].

La ANPD sancionó al BCP con una multa acumulada de S/ 289,800 (63 UIT) debido a la recopilación y almacenamiento desproporcionado de datos biométricos faciales de los usuarios que presentaban un reclamo a través del Libro de Reclamaciones Virtual. En primer lugar, la entidad bancaria recolectaba imágenes del DNI y del rostro de los reclamantes para procesarlas con validación biométrica, sin que esta medida fuera estrictamente necesaria para la finalidad de identificar al usuario (configurando así una infracción grave conforme a los artículos 7 y 28.3 de la LPDP. Además, almacenaba estos datos biométricos en su propia base de datos sin el consentimiento expreso de los titulares, lo que vulnera los artículos 5 y 13 de la LPDP, así como los artículos 7 y 12 de su Reglamento[62].

Ante estos hechos, la ANPD ordenó al BCP eliminar los patrones biométricos obtenidos, cesar el almacenamiento y evitar el uso de estos datos en futuras validaciones de identidad. Si bien se reconoce la importancia de mecanismos de seguridad en las operaciones financieras, la ANPD enfatizó que las entidades deben evaluar alternativas menos intrusivas y limitar el uso de datos biométricos a situaciones donde su tratamiento sea estrictamente necesario, pertinente y adecuado. Este caso evidencia la importancia del principio de proporcionalidad y la necesidad de que las entidades privadas se adhieran a los límites establecidos por la normativa de protección de datos personales[63].

---

[61] Resolución Directoral N°2271-2024-JUS/DGTAIPD-DPDP. EXP.N° 122-2023-JUS/DGTAIPD-PAS.

[62] Ministerio de Justicia y Derechos Humanos, “MINJUSDH sanciona a entidad financiera por inadecuado tratamiento de datos personales biométricos solicitados a sus usuarios”, Gob.pe, 6 de enero de 2025, https://www.gob.pe/institucion/minjus/noticias/1086705-minjusdh-sanciona-a-entidad-financiera-por-inadecuado-tratamiento-de-datos-personales-biometricos-solicitados-a-sus-usuarios

[63] Resolución Directoral N°110-2024-JUS/DGTAIPD. EXP.N°122-2023-JUS/DGTAIPD-PAS.

Este caso evidencia cómo el uso de datos biométricos por parte de entidades privadas puede ser desproporcionado si no se ajusta al principio de proporcionalidad. Esto nos lleva a cuestionarnos si otras instituciones, especialmente en el ámbito laboral, aplican criterios similares al requerir la identificación o autenticación de los trabajadores. ¿Se respeta el límite entre una medida legítima de seguridad y una exigencia excesiva? Esta interrogante abre el debate sobre la necesidad de garantizar un equilibrio entre la protección de la identidad y el respeto a los derechos fundamentales.

2.3.3. La inteligencia artificial en la vigilancia y recopilación de datos

2.3.3.1. Tecnologías de inteligencia artificial utilizadas en la videovigilancia

Las cámaras de circuito cerrado de televisión (en adelante CCTV) se han consolidado como una herramienta eficaz para la prevención y control del delito, partiendo del principio de que la posibilidad de ser grabados y posteriormente identificados disuade a los delincuentes de cometer actos ilícitos. En los últimos años, la IA ha adquirido un rol crucial en la optimización de la videovigilancia, facilitando el análisis avanzado de datos. Sistemas de reconocimiento facial, vinculados a bases de datos, han permitido la identificación y captura de delincuentes en países como Japón, Singapur e India[64].

En Perú, la implementación de tecnologías de inteligencia artificial en la seguridad pública ha avanzado significativamente, integrándose en sistemas de monitoreo en tiempo real. Más allá del reconocimiento facial, estas herramientas incluyen análisis predictivo del delito y centralización de datos, creando un ecosistema de vigilancia automatizado. Para maximizar su efectividad, resulta esencial definir indicadores y analizar tendencias delictivas, lo que permite reemplazar los enfoques tradicionales basados en "hot spots" por estrategias proactivas con modelos predictivos basados en datos históricos[65].

---

[64] María Moreno Jorge, Jorge Ivan Porras Aragón, Carlos Marco Céspedes Gonzales, "Uso de herramientas tecnológicas para la prevención del crimen", *Revista Académica de la Escuela de Posgrado de la Policía Nacional del Perú 3*, no.1 (2023): 37-38.

[65] Moreno, Porras Aragón Y Céspedes Gonzales, U*so de herramientas tecnológicas para la prevención del crimen*, 38.

La videovigilancia, en el Perú , ha dejado de ser un mero recurso pasivo de monitoreo para convertirse en un complejo sistema interconectado que, impulsado por la IA, redefine la seguridad y el control en las ciudades. Actualmente, extensos sistemas de videovigilancia, como el de China, cuentan con millones de cámaras equipadas con reconocimiento facial e IA, permitiendo un monitoreo automatizado y en tiempo real. Si bien el Perú aún no alcanza estos niveles de implementación, normativas como el Decreto Legislativo 1218 han sentado las bases para la consolidación de un sistema de videovigilancia interconectado en sus principales ciudades.[66].

El marco normativo que regula la videovigilancia en el Perú está constituido principalmente por el Decreto Legislativo 1218 y la Ley 30120, conocida como la Ley de Apoyo a la Seguridad Ciudadana con Cámaras de Videovigilancia Públicas y Privadas (en adelante LSCVPP). Esta regulación debe integrarse con los principios básicos sobre los derechos de la personalidad establecidos en el Código Civil como la dignidad, la intimidad y la propia imagen, así, así como con la LPDP y su reglamento. En conjunto, estas normativas tienen como propósito abordar y resolver los conflictos y desafíos jurídicos derivados de la implementación de sistemas de videovigilancia en distintos entornos sociales y comerciales.

El Decreto Legislativo N° 1218 regula el uso de cámaras de videovigilancia en bienes de dominio público, definiéndolos como aquellos destinados al uso colectivo, cuya administración, conservación y mantenimiento está a cargo de una entidad estatal. Esta normativa establece que las personas jurídicas de derecho público que posean o administren estos sistemas deben garantizar la reserva de las imágenes, videos o audios captados, salvo en casos donde existan indicios razonables de la comisión de un delito o falta, lo que obliga a informar a la Policía Nacional del Perú o al Ministerio Público para que actúen dentro de sus competencias[67].

---

[66] Javier André Murillo Chávez, “Brace yourselves! La videovigilancia ya viene:situación de la videovigilancia en el ordenamiento jurídico peruano”, *Derecho PUCP,* no. 83 (2019): 135. https://doi.org/10.18800/derechopucp.201902.005.

[67] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 033-2022-JUS/DGTAIPD, de 2 de septiembre de 2022, se refiere a la accesibilidad a la información contenida en las grabaciones de las cámaras de videovigilancia de las entidades públicas, y si estas pueden contener información de carácter secreto, reservado o confidencial.

En cuanto al acceso a la información, la Opinión Consultiva N°033-2022-JUS/DGTAIPD reafirma el deber de confidencialidad que deben mantener quienes operan los sistemas de videovigilancia en espacios públicos respecto al contenido de las grabaciones. El acceso a esta información sólo es permitido mediante orden judicial o cuando resulte necesario para la investigación de delitos. Además, establece que la entrega de esta información a las autoridades no implica la pérdida de su naturaleza reservada, trasladándose la responsabilidad de custodia a dichas entidades, que podrán ser sancionadas administrativamente o enfrentar acciones legales si incumplen esta obligación[68].

El Decreto Legislativo N° 1218 complementa la Ley N° 30120, que promueve el uso de cámaras de videovigilancia para reforzar la seguridad ciudadana. Esta ley permite que las imágenes captadas en espacios públicos por sistemas privados puedan integrarse al Sistema Nacional de Seguridad Ciudadana en casos de presunta comisión de delitos. Posteriormente, el Decreto Supremo N° 007-2020-IN precisó los procedimientos y responsabilidades para asegurar que la implementación de estos sistemas respete los derechos fundamentales de las personas, contribuyendo de manera efectiva a la prevención y persecución del delito[69].

Sin embargo, el uso de cámaras de videovigilancia no se limita únicamente a los espacios públicos. En el ámbito laboral, su implementación ha cobrado relevancia como una herramienta para la fiscalización del desempeño de los trabajadores y la seguridad dentro de las instalaciones. Si bien estas medidas pueden justificarse en función de la protección de bienes y personas, su aplicación debe armonizarse con el derecho a la privacidad y la protección de datos personales de los empleados[70].

---

[68] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 033-2022-JUS/DGTAIPD, de 2 de septiembre de 2022, se refiere a la accesibilidad a la información contenida en las grabaciones de las cámaras de videovigilancia de las entidades públicas, y si estas pueden contener información de carácter secreto, reservado o confidencial.

[69] Edhin Campos Barranzuela, “Cámaras de vigilancia en el Perú”, Lp Pasión por el Derecho, 9 de julio de 2019, https://lpderecho.pe/camaras-vigilancia-peru-edhin-campos-barranzuela/

[70] Tribunal Constitucional. EXP.N° 02208-2017-PA/TC, de 25 de septiembre de 2020, se refiere a la correcta implementación de cámaras de vigilancia en las empresas debe respetar los derechos de los trabajadores, ubicándose únicamente en áreas de libre tránsito y no en espacios privados.

La ANPD, a través de la Directiva N° 01-2020-JUS/DGTAIP, menciona que el tratamiento de datos personales mediante videovigilancia debe cumplir con los principios establecidos en dicha directiva. Según el principio de proporcionalidad, la recolección de imágenes debe ser adecuada, pertinente y no excesiva en relación con su finalidad legítima, y solo es válida si no existe un método menos invasivo que logre el mismo propósito. Asimismo, el principio de calidad exige que los datos se conserven únicamente por el tiempo necesario para cumplir su finalidad. Finalmente, respecto a los derechos de terceros, se debe evitar captar imágenes de personas ajenas al objetivo de la vigilancia. En espacios privados, las cámaras no deben grabar áreas públicas, salvo que sea indispensable, limitándose al mínimo necesario[71].

2.3.3.2. La imagen como bien jurídico protegido y su vínculo interdisciplinario con la videovigilancia

La identidad del ser humano constituye un aspecto fundamental de su existencia y puede ser representada gráficamente a través de distintos medios, como la pintura, la fotografía o la videograbación. Estos soportes, sean físicos o digitales, permiten la reproducción de la imagen de una persona en forma estática o dinámica, lo que genera la necesidad de su tutela jurídica en determinadas circunstancias. La protección del derecho a la imagen no se limita exclusivamente al rostro, sino que también abarca elementos que permitan identificar a una persona, como su vestimenta, rasgos distintivos o partes del cuerpo[72].

En este contexto, la videovigilancia adquiere particular relevancia, ya que su capacidad para registrar detalles mínimos puede derivar en la identificación de individuos sin necesidad de una captación frontal del rostro. Dado que la imagen de una persona es un bien jurídicamente protegido, su uso y tratamiento deben ser regulados para garantizar el respeto a la privacidad y la tutela de otros derechos fundamentales.

---

[71] Directiva N° 01-2020-JUS/DGTAI-PD, de 16 de enero de 2020, Tratamiento de Datos Personales mediante Sistemas de Videovigilancia. (Lima, 17 de marzo de 2020).

[72] Javier André Murillo Chávez, “Brace yourselves! La videovigilancia ya viene:situación de la videovigilancia en el ordenamiento jurídico peruano”, *Derecho PUCP,* no.83 (2019): 136. https://doi.org/10.18800/derechopucp.201902.005.

2.4. Datos biométricos y su impacto en el ámbito laboral

2.4.1. Protección de los derechos laborales frente a la recopilación biométrica

En la actualidad, el uso de tecnologías biométricas en el ámbito laboral ha generado importantes debates en torno a la protección de los derechos fundamentales de los trabajadores. La recopilación de datos biométricos como huellas dactilares, reconocimiento facial, escaneo del iris o voz, se han implementado en diversos entornos laborales con fines de identificación, control de acceso y registro de asistencia. Sin embargo, su utilización plantea serios desafíos en materia de privacidad, seguridad de la información y posibles vulneraciones a los derechos laborales.

La aplicación de los derechos fundamentales dentro de la relación laboral es el resultado de dos procesos normativos de relevancia jurídica. En primer lugar, la constitucionalización de los derechos laborales, cuyo propósito es brindar protección al trabajador, al ser la parte más vulnerable en la relación de empleo. En el marco normativo peruano, algunos ejemplos de esta protección incluyen la prioridad en el pago de la remuneración frente a otras obligaciones del empleador (artículo 24 de la Constitución Política del Perú), el derecho a la libertad sindical (artículo 28), el derecho a la huelga (artículo 28), y la protección contra el despido arbitrario (artículo 27), entre otros[73].

En segundo lugar, el proceso de la laboralización de los derechos fundamentales, los cuales permiten que estos se conviertan en mecanismos de protección para los trabajadores dentro del ámbito laboral. En este contexto, derechos como la intimidad, la privacidad y la protección de datos personales adquieren especial importancia, sobre todo frente al uso de sistemas biométricos para el control de asistencia y supervisión. Dado que estos mecanismos implican el tratamiento de datos sensibles, surge la necesidad de considerar cómo su implementación puede impactar en la esfera personal del trabajador.

---

[73] César Puntriano, "La videovigilancia en el ámbito laboral", en *El Derecho del Trabajo y la Seguridad Social en época de cambios* (Lima: Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social, 2020), 728.

A pesar de que la normativa ha reconocido ciertos límites en el uso de la videovigilancia en el ámbito laboral, no existe un desarrollo normativo específico ni jurisprudencial que regule de manera clara la implementación de sistemas biométricos, como el registro de asistencia mediante huella dactilar. Esta ausencia de regulación plantea interrogantes sobre la adecuada armonización entre el derecho del empleador a supervisar el cumplimiento de la jornada laboral y los derechos fundamentales del trabajador, en especial su privacidad y protección de datos personales.

En el contexto de la legislación peruana, los principios de protección de datos personales establecidos en la LPDP también se aplican en el ámbito laboral. No obstante, una característica particular es que el empleador, en la mayoría de los casos, no necesita el consentimiento del trabajador para el tratamiento de sus datos, siempre que dicho tratamiento se justifique dentro del contrato de trabajo y respete principios como el deber de información, proporcionalidad y seguridad. En contraste, si los datos personales se utilizan con fines ajenos a la relación laboral, como actividades publicitarias, sí será necesario obtener el consentimiento expreso del trabajador[74].

Sin embargo, esto plantea una cuestión relevante: ¿la recopilación de datos biométricos, como la huella dactilar, se ajusta a estos criterios? Si bien su uso podría justificarse para la gestión del control de asistencia, cabe preguntarse si su tratamiento respeta realmente el principio de proporcionalidad y si los trabajadores brindan un consentimiento válido e informado en este contexto.

2.4.2. Facultades del empleador para el uso de los biométricos

La relación laboral se caracteriza por una constante tensión entre el poder de dirección del empleador y los derechos fundamentales del trabajador. Según la doctrina y la jurisprudencia, el contrato de trabajo es un acuerdo por el cual una persona (trabajador) presta sus servicios de manera remunerada bajo la organización y dirección de otra (empleador)[75].

---

[74] Moore, *El derecho fundamental a la protección de datos personales en el entorno labora*l, 15

[75] César Puntriano, "La videovigilancia en el ámbito laboral", en *El Derecho del Trabajo y la Seguridad Social en época de cambios* (Lima: Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social, 2020), 724.

En la actualidad, la relación laboral se ha transformado con la incorporación de las nuevas tecnologías y la recopilación de datos biométricos, lo que ha reforzado el control empresarial sobre los trabajadores. El uso de sistemas de reconocimiento facial, huellas dactilares o identificación por retina para el registro de asistencia ha reemplazado métodos tradicionales, automatizando la fiscalización de horarios y reduciendo la necesidad de supervisión presencial[76].

El uso de la huella dactilar como mecanismo de registro de jornada laboral se ha vuelto una práctica habitual en diversas empresas. No obstante, esto plantea inquietudes en relación con la protección de los derechos de los trabajadores, especialmente en ausencia de representación sindical o de información clara por parte del empleador sobre el propósito y destino de los datos recopilados.. En tales circunstancias, el empleador goza de plena discrecionalidad para determinar el sistema de control de asistencia a implementar, sin que necesariamente deba ajustarse al principio de proporcionalidad. Asimismo, si no existen disposiciones específicas en un convenio colectivo o acuerdo laboral, la responsabilidad sobre la organización, implementación y documentación del control de jornada recae exclusivamente en la empresa. Esta situación podría comprometer las garantías de los trabajadores respecto al uso de sus datos biométricos[77].

Cabe recordar que el hecho de formar parte de una relación laboral no implica la renuncia a los derechos individuales, sino que estos se mantienen vigentes junto con aquellos propios del ámbito del trabajo. Sin embargo, la naturaleza subordinada de esta relación conlleva ciertas obligaciones, como el cumplimiento de horarios y normas internas, motivo por el cual el empleador implementa sistemas biométricos para el control de asistencia. Si bien estas medidas buscan optimizar la gestión laboral, su implementación puede llegar a ser excesiva considerando la finalidad para la cual fueron instaladas.

---

[76] Lucía Aragüez Valenzuela, "Debates emergentes en materia laboral y de privacidad: Sistemas de videovigilancia, algoritmos digitales e identificación biométrica de la persona trabajadora", *THEMIS Revista De Derecho*, no.79 (2021): 456. https://doi.org/10.18800/themis.202101.026.

[77] Valenzuela, *Debates emergentes en materia laboral y de privacidad: Sistemas de videovigilancia, algoritmos digitales e identificación biométrica de la persona trabajadora*, 459.

2.5. Marco normativo nacional e internacional

2.5.1. Análisis de la jurisprudencia peruana en materia biométrica

Es importante empezar diciendo que en el Perú, actualmente, no existe mucha jurisprudencia en relación a la protección de datos biométricos o su vulnerabilidad con respecto a su uso en el sector laboral o en la vigilancia ciudadana. Esto ocurre ya que la tecnología biométrica y su uso, son relativamente nuevos en el país y por lo tanto no es tan común que se emplee en los sectores empresariales o de vigilancia ciudadana, es algo que se ha tenido que ir desarrollando poco a poco y, por este motivo, las leyes que lo controlan también son poco específicas en ese aspecto. Podemos enumerar algunas de las causas:

1. Infraestructura tecnológica limitada: Muchas instituciones y empresas aún no han implementado sistemas biométricos debido a costos elevados y falta de equipos adecuados.

2. Acceso a internet y digitalización: En zonas rurales y alejadas, la conectividad es baja, lo que dificulta la integración de sistemas biométricos en servicios públicos y privados.

3. Costos de implementación: La tecnología biométrica requiere inversión en hardware (escáneres de huellas, reconocimiento facial, etc.) y software especializado, lo que puede ser costoso para muchas entidades.

4. Normativas y regulaciones: Aunque el Estado peruano ha impulsado el uso de biometría en algunos sectores (como el DNI electrónico y bancos), aún falta una legislación más amplia que promueva su adopción en todas las industrias.

5. Desconfianza y privacidad: Algunas personas desconfían del uso de sus datos biométricos por temor a fraudes o mal uso de la información personal.

6. Falta de capacitación: El personal que maneja estos sistemas necesita entrenamiento, y no todas las instituciones han priorizado esta inversión.

A pesar de todo esto, se encontró algunos casos con relación al uso de seguridad biométrica como los siguiente:

a. Resolución Directoral N° 2629-2022-JUS/DGTAIPD-DPDP[78]

Empezamos analizando la Resolución Directoral Nº 2629-2022-JUS/DGTAIPD-DPDP, en la cual se evaluó una denuncia presentada por el ciudadano Miguel Enrique Morachino Rodríguez contra la Municipalidad Distrital de La Victoria por presuntas irregularidades en el tratamiento de datos personales a través de su sistema de videovigilancia con reconocimiento facial donde veremos los antecedentes del caso, el proceso administrativo seguido, los hallazgos de la fiscalización y la resolución adoptada por la Dirección de Protección de Datos Personales.

El 16 de octubre de 2020, el denunciante presentó una queja ante la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD) en la que expuso preocupaciones respecto a la instalación de cámaras de videovigilancia con reconocimiento facial en el distrito de La Victoria. Entre las principales deficiencias se mencionaron:

- Falta de protocolos de confidencialidad y seguridad en el tratamiento de las imágenes captadas.
- Ausencia de información sobre el almacenamiento y tiempo de retención de los datos.
- Falta de transparencia en la transferencia de datos a otras entidades.
- Carencia de medidas de seguridad y documentación sobre autorizaciones y funciones del personal a cargo.

Tras la denuncia, la Dirección de Fiscalización e Instrucción (DFI) solicitó información a la Municipalidad Distrital de La Victoria, sin obtener una respuesta inicial satisfactoria. Luego de varias notificaciones y prórrogas, se llevó a cabo una fiscalización remota el 14 de abril de 2021, donde se encontraron las siguientes irregularidades:

[78] Dirección de Protección de Datos Personales. Resolución Directoral N° 2629-2022-JUS/DGTAIPD-DPDP, de 14 de julio, se refiere a la falta de transparencia y medidas de seguridad en el manejo de datos personales mediante un sistema de videovigilancia con reconocimiento facial instalado en el distrito.

- Uso del software "EZ STATION 3.0" para el tratamiento de imágenes, con asignación de usuarios y privilegios sin documentación formal.
- Empleo del sistema "Anyvision 1.24.0" para reconocimiento facial, sin operatividad efectiva debido a problemas técnicos y ausencia de convenio con la Policía Nacional del Perú.
- Almacenamiento de imágenes en dispositivos "NVR" por un periodo de 30 días, con acceso restringido a la Policía y al Ministerio Público mediante solicitud formal.
- Falta de procedimientos documentados sobre la gestión de accesos y revisión periódica de privilegios de usuario.

Luego del análisis de los hallazgos, la Dirección de Protección de Datos Personales determinó que la municipalidad incurrió en una infracción leve, conforme al literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP. Como consecuencia, se le impuso una multa de 1,84 Unidades Impositivas Tributarias (UIT) y se ordenó la implementación de las siguientes medidas correctivas:

- Documentar los procedimientos de gestión de accesos y revisión periódica de privilegios.
- Implementar medidas de seguridad para el tratamiento de datos personales en el sistema de videovigilancia.
- Cumplir con estas medidas en un plazo de 55 días hábiles, bajo riesgo de un nuevo procedimiento sancionador en caso de incumplimiento.

El caso refleja la importancia del cumplimiento de la normativa de protección de datos personales en el uso de tecnologías de videovigilancia por parte de las entidades públicas. La resolución destaca la necesidad de contar con protocolos claros y documentados para la gestión de datos sensibles, así como de garantizar la transparencia en el acceso a la información. La imposición de una multa y la exigencia de medidas correctivas buscan reforzar la protección de la privacidad y los derechos de los ciudadanos ante el uso de tecnologías de vigilancia.

b. Corte Suprema de Justicia de la República Sala Penal Permanente R. N. N.° 300-2021 Cusco 10 de Noviembre del 2021[79]

El siguiente caso que se examinará, tomando como referencia la jurisprudencia peruana, es el relacionado con el recurso de nulidad presentado por Jhon William Villafranca Fernández contra la sentencia dictada el 28 de febrero de 2020. Dicha resolución lo declaró culpable como autor del delito contra el patrimonio en la modalidad de robo agravado, contemplado en el artículo 188 del Código Penal. La defensa del acusado solicita que se anule todo el proceso desde la fase de instrucción, así como la sentencia, argumentando la existencia de irregularidades graves y omisiones en los procedimientos y garantías legales.

Entre los argumentos presentados para impugnar esta resolución se destaca la ausencia de un análisis biológico comparativo entre la sangre y los cabellos encontrados en las prendas halladas en la escena del crimen y las muestras del acusado. Asimismo, se cuestiona la validez del reconocimiento realizado mediante fotografías, pues no se ajustó a criterios técnico-científicos, dado que no se empleó una base de datos biométrica ni se contó con la presencia de la defensa del procesado durante el procedimiento.

En este caso podemos darnos cuenta que, aunque el uso de la tecnología de datos biométricos forma parte del sistema de justicia peruano, al tener una base de datos de los mismos, esta no fue utilizada en el proceso de sentencia del delito que es objeto de análisis. Por lo tanto el problema es que no se confirmó la identidad del imputado y sin embargo, este terminó siendo acusado, las principales pruebas en su contra que lo señalan como autor del delito se basan fundamentalmente en los testimonios presentados durante la etapa de juicio oral, por lo tanto existió una omisión en el uso del reconocimiento biométrico.

[79] Corte Suprema de Justicia de la República, Sala Penal Permanente R. N. N.° 300-2021, de 10 de Noviembre, se refiere a la omisión en el uso de reconocimiento biométrico para la adecuada identificación de un presunto acusado por el delito de robo dentro de una empresa.

Además, también nos mencionan en la sentencia que la identificación de la persona a partir de sus rasgos físicos no puede ser contrastada con la información de la ficha de Reniec, ya que está únicamente contiene una imagen del rostro, por lo tanto, dicha descripción no debería considerarse un elemento determinante en este caso, ya que esto contribuye a distorsionar la objetividad del reconocimiento.

Podemos concluir entonces que, aunque la tecnología en materia de reconocimiento biométrico existe desde hace ya algunos años en Perú, está no es usada adecuadamente o es nulo su aprovechamiento, debido también a la falta de normas que la puedan hacer obligatoria, si es que tendrá una aplicación frecuente en el futuro. Las únicas normas, en el país, relacionadas a derechos humanos en el cumplimiento de la protección de estos datos son algo ambiguas y no abarca algunos aspectos modernos, como el uso de tecnologías de IA, que podrían ser cada vez más utilizadas en la actualidad.

En ese sentido, la norma más importante es la LPDP[80], ya que es la norma superior que busca la protección de datos personales y su adecuado manejo además está respaldada por la Autoridad de Transparencia, Acceso a la Información y Protección de Datos Personales. También es importante decir que en el país los datos biométricos son considerados “datos sensibles” dentro de esta legislación, es por este motivo que están clasificados en un nivel máximo de protección y por lo tanto deben de estar adecuadamente resguardados.

Esto significa que entidades como bancos, notarías o las empresas de telecomunicación que emplean terminales para registrar datos biométricos, están obligados a mantener niveles de seguridad óptimos y a disponibilizar medios para que los usuarios puedan saber cómo se tratan sus datos y puedan ejercer los derechos ARCO[81].

[80] Ley N°29733-2024, 30 de Noviembre Ley de Protección de Datos Personales de Perú (Lima, 30 de noviembre de 2024).

[81] Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 032-2021-JUS/DGTAIPD, de 17 de agosto, se refiere a los datos biométricos y su empleo en la identificación de personas, el tratamiento de datos personales, la obtención del consentimiento, la conservación de documentos digitales, la atención de derechos ARCO.

Ahora bien, volviendo al tema de las instituciones peruanas en materia de normativa de datos biométricos, esta aplica de manera diferente en el caso de las entidades públicas en donde, si bien el cumplimiento también es obligatorio, este puede dejar de observarse en las situaciones anteriormente mencionadas. Lamentablemente no existe suficiente material normativo que desarrolle de forma más amplia el contenido de estas excepciones, salvo un pronunciamiento reciente de la ANPD personales que reafirma que, en principio las entidades del sector público deben cumplir con los mismos estándares de la LPDP, lo que incluye crear y mantener medidas de seguridad para evitar la vulneración de los datos personales recopilados y ser pasibles de sanciones administrativas si no lo hacen[82].

Podemos decir entonces que, el nivel de cumplimiento de las normas que protegen derechos humanos en materia biométrica podrían estar comprometidos por las prácticas del sector público, ya que su normativa no es muy clara. "Si bien no existen precedentes de abuso o casos públicos en donde se haya probado la violación del consentimiento en el uso de los datos personales de algún ciudadano, eso no significa que no estén ocurriendo y no sean de conocimiento público"[83]. Y se debe tomar en cuenta que también existen peligros inherentes al uso intrusivo de algunas iniciativas que buscan fortalecer la seguridad ciudadana a costa de la inseguridad de la privacidad.

La institución que desde 1993 se encargaba de la identificación biométrica en el país es el Registro Nacional de Identificación y Estado Civil (en adelante RENIEC) cuyo esquema organizativo le ha permitido centralizar todas las bases de datos biométricos del país, sobre las cuales ofrece servicios al Estado y a los particulares.

---

[82] Autoridad Nacional de Protección de Datos Personales, *El Derecho Fundamental a la Protección de Datos Personales: Guía para el Ciudadano* (Lima: Ministerio de Justicia y Derechos Humanos, 2013), https://cdn.www.gob.pe/uploads/document/file/1401558/El%20derecho%20fundamental%20a%20la%20protecci%C3%B3n%20de%20datos%20personales.pdf.

[83] Carlos Guerrero y Martín Borgioli, "Identidad Biométrica en Perú", Hiperderecho, 6 de junio de 2018, https://hiperderecho.org/wp-content/uploads/2018/06/identidad_biometrica_peru_2018.pdf

En apariencia, la forma en que RENIEC ha venido trabajando la implementación de la tecnología biométrica está acorde a usos y prácticas internacionales. Pero no existe una entidad o actores relevantes que se puedan encargar de medir el impacto de las decisiones de RENIEC en temas de biometría, por lo tanto puede estar susceptible a posibles fallos y vulnerabilidades que no son ni serán públicos, impidiendo su regulación y fiscalización.

Es necesario entonces consultar los términos generales para la protección de datos personales en el país, la cual nos dice que el objetivo de la ley es garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

2.5.2. Análisis de la doctrina y jurisprudencia extranjera sobre materia biométrica

2.5.2.1 España

Cuando hablamos de utilización de medios biométricos para el control laboral de los trabajadores, debe existir un análisis previo en donde se pueda notar la necesidad de usar dichas tecnologías biométricos en las empresa, descartando que no exista otro medio igual de eficaz y menos intrusivo, antes de la implantación de cualquier sistema, en el cual debe existir un análisis de riesgos adecuado y superarse la evaluación de impacto teniendo en cuenta el triple juicio de idoneidad, necesidad y proporcionalidad[84].

Con ello, lo que se busca es encontrar un equilibrio entre el desarrollo tecnológico y la protección de los derechos y libertades de las personas, especialmente en el derecho fundamental de protección de datos personales.Teniendo en cuento ello, a continuación, desarrollaremos una jurisprudencia española que habla del tema:

---

[84] María Loza, Patricio Monreal, “Biometría en el Entorno Laboral”, *Govertis (blog),* 12 de diciembre 2023, https://www.govertis.com/biometria-en-el-entorno-laboral

a. Juzgado de lo Social N°. 2 de Alicante/Alacant, Sentencia 190/2023 de 15 Sep. 2023, Rec. 489/2023[85]

El caso analizado correspondiente a la Sentencia 190/2023 del Juzgado de lo Social N° 2 de Alicante establece un precedente relevante en la regulación del uso de datos biométricos en el ámbito laboral. La resolución judicial confirma la vulneración de los derechos fundamentales de un trabajador, el señor Gabino, por parte de la empresa Albero Forte Composite al implementar un sistema de fichaje basado en el reconocimiento facial sin su consentimiento específico ni una evaluación de impacto en protección de datos personales.

El trabajador prestó servicios para la empresa bajo un contrato de duración determinada, vigente del 18 de marzo al 17 de abril de 2022. Durante su periodo laboral, la empresa implementó un sistema de fichaje basado en reconocimiento facial, que implicaba la toma de fotografías de los empleados al ingresar y salir del centro de trabajo. En este contexto, el 17 de marzo de 2022 se le tomó una fotografía con el propósito de ser utilizada en diversos medios. Sin embargo, no se le informó de manera detallada sobre el tratamiento de sus datos personales más allá de lo estipulado en el documento que firmó.

El señor Gabino sostiene que nunca se le informó sobre el fin que le darían a sus datos biométricos y que únicamente se le solicitó firmar un consentimiento relacionado con el uso de sus derechos de imagen. Dicho documento autorizaba a la empresa a emplear y difundir su imagen en su página web, redes sociales, campañas, revistas, folletos, publicidad en beneficio de la empresa y otros materiales promocionales. No obstante, el trabajador no brindó un consentimiento explícito para el tratamiento de sus datos biométricos, ya que el documento suscrito únicamente autorizaba el uso de su imagen conforme a los fines previamente señalados por la empresa.

[85] Juzgado de lo Social N° 2 de Alicante. Sentencia N° 190/2023, de 15 de septiembre, se refiere al reconocimiento facial con objeto del control laboral.

Ante esta situación, el trabajador presentó un reclamo ante la Agencia Española de Protección de Datos (en adelante AEPD) argumentando que su imagen estaba siendo utilizada sin su consentimiento para el control de asistencia laboral, es por ello por lo que la AEPD determinó que la empresa había incurrido en una infracción grave al no haber realizado una evaluación de impacto en protección de datos previa a la implementación del sistema biométrico.

Así, el Juzgado de lo Social N° 2 de Alicante concluyó que la empresa había vulnerado los derechos fundamentales del trabajador, particularmente el derecho a la intimidad y a la propia imagen. En consecuencia de ello, la sentencia determinó que se realice el cese inmediato del uso del reconocimiento facial como método de fichaje en la empresa y el pago de una indemnización de 6,251 euros al trabajador por concepto de daños morales.

Teniendo en cuenta aquello, para este caso, se ha considerado que la protección de los datos biométricos en Europa y España está regulada principalmente por el Reglamento General de Protección de Datos (en adelante RGPD), el cual es el Reglamento (UE) 2016/679 que establece en su artículo 9 la prohibición del tratamiento de datos biométricos salvo algunas excepciones como el consentimiento explícito del interesado o razones de interés público[86].

Por otro lado, este país cuenta con la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, el cual complementa el RGPD en el ordenamiento español, destacando así la necesidad de evaluar la proporcionalidad de estos sistemas en el ámbito laboral[87]. Este fallo lo que enfatiza es la falta de proporcionalidad en el uso del reconocimiento facial ya que la empresa podía haber implementado métodos menos intrusivos como tarjetas de acceso o códigos QR.

[86] Reglamento (UE) 2016/679, de 27 de abril, Reglamento General de Protección de Datos. (Unión Europea, 5 de mayo de 2016).
[87] Ley Orgánica 3/2018, de 5 de diciembre, Ley de Protección de Datos Personales y Garantía de los derechos digitales. (Madrid, 6 de diciembre de 2018).

2.5.2.2 Brasil

Brasil es considerado uno de los países con mejor marco jurídico en materia de protección de datos personales, incluyendo los datos biométricos. En este sentido la principal legislación en materia de protección de datos es la Ley General de Protección de Datos (LGPD - Lei Geral de Proteção de Dados, Ley N° 13.709/2018)[88]. La protección de los datos biométricos en Brasil es un tema de creciente importancia, dado su impacto en la privacidad; su normativa busca equilibrar la transparencia y la seguridad con los derechos individuales. Esto es clave ante el uso de tecnologías de identificación y monitoreo.

Esta ley es aplicada a cualquier operación de tratamiento de datos personales, así como datos biométricos realizada en Brasil o que afecte a personas en el país, incluso si la empresa responsable de recabar esos datos está fuera de este país. Las personas que acceden a proporcionar estos datos a las empresas tienen en esta ley el derecho a acceder, corregir, eliminar y portar sus datos personales, además de restringir su tratamiento, para ello cuentan con la Autoridad Nacional de Protección de Datos (ANPD)[89] quien es el organismo encargado de supervisar y garantizar el cumplimiento de la ley general de protección de datos.

Además de la ley antes mencionada, existe otra relacionada a la protección de datos en el país sudamericano y es la Ley de Acceso a la Información (Ley N° 12.527/2011) la cual establece normas que buscan garantizar la transparencia y el acceso a la información pública en este país, entró en vigor el 16 de mayo de 2012 y se basa en el principio de que el acceso a la información es un derecho fundamental de los ciudadanos y una obligación del Estado.[90]

En cuanto a la jurisprudencia de este país, podemos mencionar la siguiente:

[88] Ley N° 13.709/2018, de 14 de agosto, Lei Geral de Proteção de Dados. (Brasil, 15 de agosto de 2020).
[89] Carlos Elizario de Lima; Lucas Gomes, "Autoridad Nacional de Protección de Datos de Brasil: estructuración e iniciativas", iapp (International Association of Privacy Professionals), 8 de septiembre de 2021, https://iapp.org/news/a/autoridad-nacional-de-proteccion-de-datos-de-brasil-estructuracion-e-iniciativas/
[90] Lei Nº 12.527/2011 - LAI, de 18 de noviembre, Lei de acesso a informaçõ pública. (Brasil, 16 de mayo de 2012)

a. Tribunal de Justiça do Estado de São Paulo (TJSP) 37ª Vara Cível do Foro Central Cível de São Paulo. N° 1090663-42.2018.8.26.0100[91]

   El caso entre el Instituto Brasileño de Defensa del Consumidor (en adelante IDEC) y ViaQuatro, concesionaria de la Línea 4-Amarilla del Metro de São Paulo, representa un hito en la protección de datos personales y los derechos de los consumidores en Brasil. La demanda fue presentada por el IDEC con el objetivo de detener la recolección no autorizada de datos biométricos de los usuarios del metro.

   Según la denuncia, ViaQuatro había instalado cámaras en siete estaciones con el propósito de recolectar imágenes faciales, sin el consentimiento previo de los usuarios, lo que se consideró una violación directa de los derechos de privacidad y protección de datos personales estipulados por la legislación brasileña. Estas cámaras se encontraban integradas en puertas digitales interactivas y se utilizaban con fines publicitarios y estadísticos, lo que incrementaba los beneficios comerciales de la concesionaria sin informar adecuadamente a los usuarios sobre la captación de sus datos personales.

   Este conflicto subraya la creciente preocupación por el uso de datos biométricos sin autorización en espacios públicos. La falta de transparencia en la recopilación de información sensible plantea serios cuestionamientos sobre el respeto a la privacidad.

   Es por tal motivo que el IDEC solicitó al tribunal la prohibición inmediata de la recolección y tratamiento de datos biométricos sin el consentimiento expreso de los usuarios. Además, exigió la desconexión de las cámaras bajo pena de una multa diaria de R$ 50.000 y la imposición de una indemnización por daños morales, así como una compensación por daños colectivos que ascendiera a un mínimo de R$ 100.000.000.

[91] Tribunal de Justiça do Estado de São Paulo (TJSP) 37ª Vara Cível do Foro Central Cível de São Paulo. N° 1090663-42.2018.8.26.0100, de 7 de mayo, se refiere a la captación de datos biométricos mediante cámaras instaladas en puertas digitales interactivas en las estaciones del metro, sin el consentimiento de los usuarios.

> La organización argumentó que la captación de imágenes sin consentimiento violaba los derechos básicos del consumidor, específicamente el derecho a la información clara y adecuada, así como la protección contra prácticas comerciales abusivas establecidas por el Código de Defensa del Consumidor de Brasil.
>
> Por su parte, ViaQuatro defendió la legalidad de sus prácticas argumentando que las cámaras no realizaban reconocimiento facial ni almacenaban imágenes, sino que sólo detectaban características generales de los rostros de los usuarios para generar datos estadísticos anónimos, tales como género, rango de edad y expresiones faciales.
>
> Según la empresa, esta información se utilizaba exclusivamente con fines estadísticos y no violaba los derechos de privacidad de los usuarios. Además, ViaQuatro alegó que la instalación de los dispositivos contaba con la autorización del gobierno, y que las actividades publicitarias generaban ingresos adicionales para la concesionaria, contribuyendo a la sostenibilidad económica del servicio de transporte público.

El tribunal concedió la tutela de urgencia solicitada por el IDEC, ordenando a ViaQuatro cesar la recolección de datos y apagar las cámaras instaladas en un plazo de 48 horas. Además, ordenó la colocación de adhesivos en las cámaras para demostrar su desconexión efectiva. La decisión judicial también rechazó el uso de pruebas de otro proceso judicial presentado por la defensa de ViaQuatro, argumentando que su aceptación violaría el principio de contradicción, ya que las partes afectadas no habían tenido la oportunidad de participar en la recolección de dicha prueba ni de presentar impugnaciones.

El fallo se basó en la Ley General de Protección de Datos (LGPD), que clasifica los datos biométricos como datos personales sensibles y exige el consentimiento explícito para su recolección y tratamiento. Según el tribunal, la mera detección facial, aunque no implique reconocimiento o almacenamiento de imágenes, ya constituye un tratamiento de datos biométricos que requiere autorización expresa por parte del usuario.

Además, el tribunal consideró que ViaQuatro no había proporcionado evidencia suficiente de que los datos recolectados no eran almacenados ni utilizados con fines comerciales más allá del análisis estadístico. Como resultado del fallo, ViaQuatro fue condenada a cesar el uso de datos biométricos sin el consentimiento explícito de los usuarios y a implementar mecanismos claros de información y obtención de consentimiento si deseaba retomar estas prácticas en el futuro.

La empresa también fue condenada a pagar una indemnización por daños morales colectivos debido a la violación de los derechos fundamentales de los usuarios del servicio público, aunque el tribunal no estableció una indemnización individualizada debido a la falta de pruebas concretas que justificaran dicha compensación.

Este caso establece un precedente importante en la protección de los derechos de los consumidores y la privacidad en Brasil, resaltando la necesidad de obtener el consentimiento explícito antes de utilizar datos personales, especialmente en el contexto de servicios públicos. La decisión también subraya el papel fundamental de las instituciones de defensa de los consumidores, como el IDEC y la Defensoría Pública, en la protección de los derechos colectivos frente a las prácticas comerciales invasivas.

2.5.2.3 México

México es otro de los países que ha avanzado en la creación de un marco legal apto para la correcta protección de datos personales. La principal legislación que rigen esta materia es Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante LFPDPPP)[92] la cual fue promulgada en el año de 2010, y en ella se establecen las bases, principios y procedimientos para el tratamiento de datos personales por parte de entidades privadas. Además de incluir conceptos como el consentimiento, los derechos ARCO y medidas de seguridad para proteger los datos personales.

[92] Ley Federal de Protección de Datos Personales en Posesión de los Particulares/2010 - de 5 de julio, LFPDPPP. (Ciudad de México, 5 de julio de 2010)

También existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[93] del año 2017, en ella se busca establecer los principios y bases para dar garantía de que se respetará el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, con esto nos referimos a las entidades gubernamentales.

Además que en México, al buscar alinearse con estándares internacionales de protección de datos, ha logrado facilitar la cooperación y el comercio con otras naciones cumpliendo con otras regulaciones en materia de protección de datos personales como lo es el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, el cual es esencial para las empresas mexicanas que operan globalmente.

Ahora bien aunque existe este tipo de marco jurídico para la protección de los datos personales en México, el principal problema que existe es que con él es necesaria la aplicación de un sistema de nuevo en el tratamiento de la información personal haciendo uso de nuevas tecnologías, y al hablar de un país como México debemos de recordar que los niveles de corrupción de los últimos años en ese país han sido elevados trayendo como consecuencia que las bases de datos biométricos puedan estar en riesgo de ser vulnerables y se haga un mal uso de las misma.

Por esa razón, para los especialistas mexicanos en esta materia, el debate no se encuentra dentro del resguardo y obtención de este tipo de datos sino más bien en encontrar las herramientas necesarias para administrarlos y resguardarlos adecuadamente. El gobierno también debe proporcionar un adecuado marco jurídico para que las personas tengan más seguridad a la hora de brindar este tipo de datos a las distintas instituciones. A continuación, hablaremos de la jurisprudencia en relación a la protección de datos en México.

Un ejemplo sobre la jurisprudencia de este país, en materia de datos biométricos lo podemos encontrar a continuación:

[93] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados/2017 - de 26 de enero, LGPDPPSO. (Ciudad de México, 26 de enero de 2017)

a. Tribunal Pleno de la Suprema Corte de Justicia de la Nación LXIV Legislatura Ciudad de México. N° 82/2021 y N° 82/2021.[94]

   En 2021, los senadores de la cámara de diputados mexicana presentaron un estricto en donde buscaban tratar como inconstitucional una ley que permitiría la recolección obligatoria de los datos biométricos de todos los ciudadanos mexicanos, sin excepción, que contaran con algún dispositivo móvil, violando los derechos a la protección de datos personales. Estos datos pretendían ser recabados por un Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) de forma indiscriminada y sin un interés legítimo acorde con los parámetros constitucionales de aquel país.

   Además de que se alegó que los datos personales exigidos por el PANAUT podrían ser fácilmente vulnerados y, debido a la información que en ellos se contiene, podrían dar paso a la aparición de delitos como el robo de identidad, robo de cuentas bancarias y datos muy personales de los ciudadanos que se encuentren dentro de este padrón.

   Es por todo esto que se declaró inválida la creación de una base de datos biométricos como la PANAUT al ser inconstitucional, con lo cual se asentó un precedente muy importante tanto para el resguardo de la información de los ciudadanos mexicanos, como para iniciativas futuras que pudieran poner en riesgo el derecho a la privacidad.

   Este es un caso interesante que nos advierte de los riesgo que existen con el manejo de la información de datos sensibles de las personas, porque incluso las instituciones gubernamentales pueden llevar a violar varios derechos y principios en materia de protección de datos personales, si es que no cuentan con un adecuado procedimiento para la obtención de los mismo.

---

[94] Tribunal Pleno de la Suprema Corte de Justicia de la Nación LXIV Legislatura Ciudad de México. N° 82/2021 y N° 82/2021, de 25 de abril, se refiere a la creación de un Padrón de datos biométricos de todo ciudadano mexicano que cuente con un dispositivo móvil activo.

2.6. Hipótesis

2.6.1. Hipótesis general

El uso del reconocimiento biométrico en la vigilancia ciudadana y el control laboral supone una vulneración al derecho a la protección de datos personales, especialmente cuando las medidas adoptadas por las entidades no garantizan de manera efectiva la autodeterminación informativa de los individuos.

2.6.2. Hipótesis específicas

a. La implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral genera riesgos para la protección de datos personales. Si bien en el ámbito de la videovigilancia existen medidas de protección, en el control laboral la falta de una regulación específica podría derivar en consecuencias jurídicas como la vulneración del derecho a la privacidad y la autodeterminación informativa.

b. En otros países, como en España, la regulación sobre la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral establecen límites estrictos para el tratamiento de datos biométricos, exigiendo principios como la proporcionalidad y la minimización de datos.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Diseño de la investigación

3.1.1. Diseño

Esta investigación será de tipo cualitativo, lo que significa que se utilizarán datos obtenidos del instrumento de medición elegido (entrevistas) para comprobar la hipótesis. Se realizaron entrevistas a especialistas en Nuevas Tecnologías y Derecho Laboral, a efectos de determinar la opinión de la muestra representativa y utilizarla como instrumento de medición.

3.1.2. Tipo - Nivel

La investigación actual es descriptiva porque este tipo de investigación se orienta hacia el conocimiento sobre la realidad presentada en una situación espacial y temporal determinada. Por ello se denomina descriptiva. He aquí, los investigadores se centraron en comprender las propiedades de los fenómenos evaluados[95]. Asimismo, considero que también posee un tipo correlacional porque busca medir el grado de relación que existe entre dos conceptos o variables en un contexto particular[96]

3.1.3. Enfoque

El enfoque de este estudio es cualitativo, en tanto se refiere el paradigma jurídico positivista, que pretende abordar el objeto de estudio por sus características y manifestaciones observables, con atención a la recolección de datos, clasificación y análisis estadístico. Nuevamente, el objetivo es medir y probar hipótesis, y si sus resultados están relacionados con variables que explican la causalidad, el objetivo será crear patrones de comportamiento y generalizaciones que estudiemos[97].

3.2. Población y muestra

3.2.1. Población objetivo

Para la presente investigación, nuestra población objetivo son los expertos en Derecho Laboral y especialistas en Nuevas Tecnologìas.

---

[95] Reynaldo Tantalean, “El alcance de las investigaciones jurídicas.” Derecho y Cambio Social, N.º 41, (2015):6
[96] Tantalean, “El alcance de las investigaciones jurídicas.” 7
[97] Augusto Ramos, Cómo hacer una tesis de Derecho y no envejecer en el intento, (Lima: Grijley, 2014) 927 – 929.

3.2.2. Método de muestra

En esta investigación, el método de muestra es no probabilístico porque no se han elegido a los individuos de forma aleatoria, teniendo una característica en común entre nuestra población. De este modo, en el proceso de muestreo se empleó el método de selección por conveniencia, eligiendo a los individuos a los que se tuvo un acceso más fácil, con el fin de obtener una muestra confiable y adecuada.

3.2.3. Tamaño de la muestra

Con el objetivo de garantizar una evaluación completa y precisa del tema abordado, se eligió una muestra conformada por cinco profesionales con especialización en Derecho Laboral y especialización en Nuevas Tecnologías. Esta selección facilita la recopilación de diversas perspectivas y permite un análisis teórico más profundo. El tamaño de la muestra se definió considerando la importancia de obtener una representación adecuada de las opiniones expertas, sin afectar la viabilidad del estudio.

3.3. Método de recolección de datos e instrumentos de medición

En esta investigación se llevaron a cabo entrevistas con expertos en el tema, en las que se plantearon diversas preguntas fundamentadas en el marco teórico elaborado. El propósito es recopilar la mayor cantidad de información posible, aprovechando la experiencia de los especialistas entrevistados. Para los instrumentos de medición, se emplearán entrevistas dirigidas a especialistas en las áreas de Nuevas Tecnologías y especialistas en Nuevas Tecnologías.

3.4. Guía de entrevista

GUÍA DE ENTREVISTA
Fecha/Hora:
Entrevistadora:
Entrevistado(a):
Somos egresadas de la Universidad ESAN con el grado de bachiller en Derecho Corporativo, y actualmente nos encontramos desarrollando un trabajo de investigación con la finalidad de optar al título profesional de abogadas.

El tema de nuestra investigación es "Reconocimiento biométrico en el Perú: Entre la vigilancia ciudadana y el control laboral". Nuestro estudio tiene como objetivo analizar el uso del reconocimiento biométrico tanto en la seguridad pública como en el ámbito laboral, evaluando sus implicancias en la protección de la privacidad y los derechos fundamentales. En particular, buscamos determinar si su implementación por parte del Estado y los empleadores se adecúa al marco legal vigente y a los principios constitucionales, o si, por el contrario, podría representar una amenaza para los derechos de los ciudadanos y trabajadores. En el marco de dicha investigación, agradeceremos que nos pueda ayudar respondiendo las siguientes preguntas:	
N°	Preguntas
1	¿Está familiarizado con la Ley N° 29733, ley que protege los datos personales? ¿Cree que debería existir una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos?
2	¿Existe asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos? ¿Considera que esta falta de transparencia limita la posibilidad de tomar decisiones informadas sobre su uso?
3	Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo considera que una violación de seguridad podría afectar la privacidad de los trabajadores en el ámbito laboral?
4	¿Qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas?¿Cuál es su opinión sobre el uso de la inteligencia artificial en las cámaras de videovigilancia en el Perú y su impacto en la privacidad de los ciudadanos?

3.5. Técnicas de recolección de datos

La técnica de recolección utilizada se basó en la realización de entrevistas a expertos en Nuevas Tecnologías y especialistas en Nuevas Tecnologías, con el objetivo de conocer sus opiniones y recopilar los conocimientos que puedan contribuir a responder las preguntas formuladas.

3.6. Técnicas para el procesamiento y análisis de la información

Dado que la información recopilada no fue extensa, no se recurrió al uso de paquetes estadísticos para su análisis.

CAPÍTULO IV: RESULTADOS DE LA INVESTIGACIÓN EMPÍRICA

4.1. Validación del instrumento

La prueba piloto se llevó a cabo el 25 de febrero del 2025 y estuvo dirigida al Abogado Carlos Jimenez Silva, quien es experto en el Campo Laboral y Seguridad Social. Las conclusiones de esta prueba indicaron que las preguntas eran adecuadas, claras y suficientes para obtener la información necesaria que complementará el marco teórico y va a permitir realizar un análisis correcto.

4.2. Resultados

De acuerdo a las incógnitas presentadas, los resultados generales de las entrevistas revelan un consenso en torno a la importancia de proteger los derechos fundamentales en el contexto del uso de tecnologías biométricas y la inteligencia artificial. Los entrevistados demostraron estar familiarizados con la Ley N° 29733, lo que indica un conocimiento básico sobre la protección de datos personales en el ámbito laboral y digital.

En cuanto a la regulación específica para la inteligencia artificial en el tratamiento de datos biométricos, la mayoría coincide en que es necesario establecer límites claros. Se destaca la idea de que los sistemas biométricos deben funcionar como herramienta auxiliar y no como sustituto de la toma de decisiones del empleador, quien debe conservar la última palabra. Además, se enfatiza la necesidad de que se informe de manera completa a los trabajadores, garantizando un consentimiento libre, informado y expreso, lo que permitiría mitigar la asimetría de información y poder entre empleador y empleado.

Respecto a la seguridad, se subraya que, dada la naturaleza permanente y única de los datos biométricos, cualquier violación de seguridad podría tener consecuencias muy graves en la privacidad de las personas. Por ello, resulta fundamental implementar altos estándares de protección y someter las medidas a un riguroso análisis de proporcionalidad. Este test de proporcionalidad exige que la medida adoptada sea idónea, necesaria y proporcional, considerando siempre la posibilidad de utilizar métodos menos invasivos que logren el mismo objetivo.

4.2.1. Tabla de Tabulación e Interpretación

Pregunta	Entrevista 1 (Carlos Jiménez Silva)	Entrevista 2 (Fátima Toche Vega)	Entrevista 3 (María Camargo Román)	Entrevista 4 (José Saul Casas Chuso)	Entrevista 5 (Lyanee Pineda Abuhadba)
1. ¿Está familiarizado con la Ley N° 29733 y cree que debe existir una regulación específica para el uso de IA en datos biométricos?	Conoce la norma y opina que la inteligencia artificial debe funcionar como herramienta de apoyo, reservando la decisión final al empleador, siempre que se establezcan límites claros y se informe de forma transparente. **Posición: De acuerdo.**	Conoce la ley y aboga por una regulación específica que detalle el tratamiento de datos biométricos, garantizando un consentimiento libre, informado y expreso. **Posición: De acuerdo.**	Conoce la norma, pero distingue entre "uso" y "entrenamiento" de datos biométricos; considera que no es imprescindible legislar específicamente para la IA, ya que el problema se centra en el acceso no autorizado. **Posición: No de acuerdo.**	Tiene conocimiento general de la norma y opina que debe promulgarse una regulación específica sobre el uso de IA en datos biométricos, tanto por razones éticas como para contrarrestar futuros inconvenientes de ciberseguridad **Posición: De acuerdo**	Conoce la ley y considera fundamental que exista una regulación específica para el uso de IA en datos biométricos, especialmente en el ámbito laboral, debido a la alta sensibilidad de estos datos y a su posible compartición con terceros. **Posición: De acuerdo.**
2. ¿Existe asimetría de información y poder cuando se recopilan datos biométricos sin el consentimiento adecuado? ¿Limita esto la posibilidad de tomar decisiones informadas?	Reconoce la asimetría inherente entre empleador y trabajador, justificándola si se establecen límites adecuados y se garantiza la transparencia. **Posición: De acuerdo.**	Afirma que existe asimetría y destaca que se puede mitigar mediante políticas claras de privacidad y un deber de información que permita decisiones informadas. **Posición: De acuerdo.**	Destaca que la falta de consentimiento agrava la asimetría, dificultando la toma de decisiones informadas y vulnerando derechos fundamentales **Posición: De acuerdo.**	Señala que la ausencia de información y de consentimiento adecuado fomenta una asimetría que posibilita el uso indebido de datos biométricos. **Posición: De acuerdo**	Sostiene que, sin un consentimiento adecuado, la asimetría de información y poder se incrementa, limitando significativamente la posibilidad de tomar decisiones informadas y generando riesgos para la privacidad. **Posición: De acuerdo.**

3. Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo afectaría una violación de seguridad la privacidad de los trabajadores?	Advierte que una violación de seguridad vulneraría la intimidad y el secreto de la información, afectando irreversiblemente datos sensibles. **Posición: De acuerdo.**	Resalta que, por la permanencia de los datos biométricos, cualquier filtración compromete gravemente la identidad y seguridad personal. **Posición: De acuerdo.**	Sostiene que la exposición de datos facilita la suplantación de identidad y afecta el acceso a servicios esenciales, incrementando el riesgo para la privacidad. **Posición: De acuerdo.**	Afirma que las violaciones de seguridad afectan tanto la esfera laboral como la privada, pudiendo derivar en fraude, robo de identidad y divulgación de información sensible. **Posición: De acuerdo.**	Considera que una violación de seguridad tendría consecuencias devastadoras para la privacidad, generando riesgos de acceso indebido, discriminación y otros perjuicios. **Posición: De acuerdo.**
4. ¿Qué medidas son necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales y cuál es su opinión sobre el uso de IA en las cámaras de videovigilancia?	Propone limitar el uso de biométricos a lo estrictamente necesario, garantizando transparencia y consentimiento informado, y aplicando el test de proporcionalidad para que la medida sea adecuada, necesaria y proporcional. Respecto a la videovigilancia, considera aceptable su uso para proteger bienes y prevenir accidentes, siempre que se evite su aplicación en zonas de intimidad. **Posición: De acuerdo.**	Recomienda un análisis riguroso de proporcionalidad que incluya altos estándares de seguridad (encriptación, retención limitada) y un consentimiento libre y expreso. Opina que la IA en videovigilancia debe estar sujeta a control judicial para prevenir vulneraciones de derechos fundamentales. **Posición: De acuerdo.**	Aboga por limitar la captación de datos biométricos a situaciones estrictamente necesarias y sugiere emplear alternativas menos invasivas cuando sea posible. Crítica la eficacia del reconocimiento facial en entornos no controlados y recomienda su uso solo en escenarios adecuadamente regulados. **Posición: De acuerdo.**	Destaca la necesidad de establecer límites y reglas claras para el uso de IA y datos biométricos, para contrarrestar riesgos de ciberseguridad. Considera factible la implementación de IA en las cámaras de videovigilancia en espacios públicos, siempre que se establezcan controles adecuados para identificar delincuentes sin vulnerar la privacidad de los ciudadanos. **Posición: De acuerdo.** **.**	Destaca la importancia de implementar políticas claras de privacidad y seguridad, obtener el consentimiento informado de manera rigurosa y establecer mecanismos para notificar y responder a incidentes de seguridad. En cuanto a la IA en videovigilancia, subraya que debe regularse estrictamente para evitar vulneraciones, especialmente en el ámbito laboral. **Posición: De acuerdo**

CAPÍTULO V: ANÁLISIS Y DISCUSIÓN DE RESULTADOS

En este apartado se llevará a cabo un análisis cualitativo basado en la información obtenida a través de las entrevistas realizadas a expertos en Nuevas Tecnologías y Derecho Laboral, complementado con el estudio de fuentes doctrinales, jurisprudenciales y normativas consultadas. Dicho análisis se desarrollará a partir de la construcción de conceptos derivados del marco teórico, los cuales serán enriquecidos con las perspectivas y valoraciones de los especialistas consultados.

El trabajo de investigación se ha desarrollado en torno a las dos variables principales del análisis: en primer lugar, el impacto del uso de cámaras de videovigilancia con inteligencia artificial en los distritos de Lima, y, en segundo lugar, la implementación de sistemas biométricos, como los sensores de reconocimiento dactilar, para el control laboral de los trabajadores. El estudio de estas variables permitirá examinar los alcances y limitaciones de estas tecnologías, así como los desafíos jurídicos que su aplicación conlleva.

Del análisis de las entrevistas realizadas, se desprende un consenso general entre los expertos sobre la relevancia del tema de investigación. No obstante, si bien existe coincidencia en ciertos puntos clave, los especialistas difieren en los argumentos que sustentan sus posturas y en las soluciones que proponen. Esta diversidad de enfoques se refleja en los resultados obtenidos a partir de las entrevistas realizadas a cinco especialistas en Nuevas Tecnologías y Derecho Laboral.

A continuación, se dará inicio al análisis de la primera variable de estudio, relacionada con la implementación de sistemas de videovigilancia con inteligencia artificial. Este apartado examinará el impacto de estas tecnologías en la seguridad y la protección de datos personales, considerando su uso en espacios públicos. En este contexto, resulta relevante analizar la implementación de cámaras con reconocimiento facial en diversas municipalidades, como La Municipalidad de El Agustino, Miraflores y Surco, las cuales han adoptado esta tecnología como parte de sus estrategias para combatir la delincuencia y el sicariato en calles, avenidas, parques y zonas de alta concurrencia. Para ello, se abordarán los aspectos normativos, jurisprudenciales y las perspectivas de los especialistas consultados, con el fin de identificar los riesgos asociados y las posibles medidas para garantizar un equilibrio entre la seguridad y la privacidad.

En este punto, también realizaremos una ponderación utilizando el instrumento del test de proporcionalidad, dado que se encuentran en colisión dos derechos constitucionalmente reconocidos: el derecho a la privacidad e intimidad y el derecho a la seguridad ciudadana. Este análisis se articulará en tres etapas: idoneidad, necesidad y proporcionalidad en sentido estricto.

El procedimiento para la aplicación del test de proporcionalidad sigue tres etapas fundamentales. En primer lugar, se realiza un juicio de idoneidad o adecuación, que consiste en determinar si la restricción de un derecho fundamental es pertinente y adecuada para alcanzar el objetivo que se pretende proteger. Superado este análisis, se procede a evaluar la necesidad de la medida, lo que implica verificar si existen alternativas menos lesivas que permitan alcanzar la misma finalidad. Este examen se basa en una comparación entre el medio elegido y otras posibles opciones que el legislador o la autoridad competente podrían haber adoptado. Finalmente, si la medida supera las etapas previas, se lleva a cabo la ponderación entre los principios constitucionales en conflicto. En esta fase, se aplica el principio de proporcionalidad en sentido estricto, según el cual, a mayor afectación de un derecho, mayor debe ser la justificación y relevancia del interés que se busca proteger[98].

1. Idoneidad: El juicio de idoneidad exige que toda medida que limite derechos fundamentales sea adecuada para alcanzar un fin constitucionalmente legítimo. En este caso, el medio utilizado es la implementación de cámaras de videovigilancia con inteligencia artificial en espacios públicos, cuyo fin legítimo es la prevención y control de la delincuencia, así como la protección de bienes y personas. No obstante, esta medida también implica una limitación del derecho a la protección de datos personales y la privacidad, debido a la recopilación y tratamiento masivo de información biométrica. Si bien estas tecnologías pueden resultar técnicamente eficaces para identificar situaciones de riesgo y detectar la presencia de individuos involucrados en actividades delictivas, su idoneidad no solo debe evaluarse desde una perspectiva operativa, sino también desde el respeto a los derechos fundamentales. Por ello, su implementación debe enmarcarse dentro de límites claros que eviten la captación indiscriminada de imágenes en zonas de esparcimiento o espacios privados dentro de la vía pública, garantizando un equilibrio entre la seguridad ciudadana y la protección de la privacidad.

[98] Sentencia del Tribunal Constitucional. EXP N°579-2008-PA/TC.

2. Necesidad: En segundo término, resulta imprescindible examinar la necesidad de la medida, lo que implica valorar si existen medios alternativos que puedan alcanzar el mismo fin de garantizar la seguridad ciudadana con un menor impacto en los derechos fundamentales. En este sentido, la identificación de métodos alternativos, como el incremento de patrullajes policiales o la instalación de sistemas tradicionales de alerta, podría ofrecer soluciones complementarias. Sin embargo, la creciente interconexión y la inmediatez que proporciona la videovigilancia automatizada con inteligencia artificial han demostrado optimizar la identificación de personas involucradas en hechos delictivos y permitir la proyección de posibles actos ilícitos con base en patrones de comportamiento. No obstante, la necesidad de estas tecnologías solo se justifica si su aplicación se circunscribe a un ámbito geográfico delimitado, con un propósito exclusivo de seguridad y sin derivar en la creación de bases de datos masivas que puedan ser utilizadas con fines ajenos a la protección ciudadana.

3. Proporcionalidad en sentido estricto: Por tercer paso tenemos, la proporcionalidad en sentido estricto, requiere un balance cuidadoso entre el beneficio en materia de seguridad y la intromisión que supone la captación y tratamiento de imágenes de diferentes personas, lo que afecta su derecho a la privacidad e intimidad.

   La implementación de cámaras de videovigilancia con inteligencia artificial constituye un medio idóneo para fortalecer la seguridad ciudadana, facilitando la identificación de individuos involucrados en actos delictivos y la prevención de incidentes en espacios públicos. No obstante, para garantizar que esta medida no resulte más lesiva de lo necesario, su aplicación debe limitarse a zonas estratégicas y de alta visibilidad, evitando su uso indiscriminado en áreas donde la expectativa de privacidad sea mayor.

   En este sentido, la Directiva N° 01-2020-JUS/DGTAIPD, que regula el tratamiento de datos personales captados mediante sistemas de videovigilancia, establece en su numeral 6.4 que el uso de estas tecnologías será legítimo únicamente si no existe un medio menos invasivo o igual de eficaz para alcanzar la finalidad perseguida. Asimismo, deben implementarse controles rigurosos para asegurar que la información recopilada se utilice exclusivamente con fines de seguridad y no derive en un mecanismo de vigilancia masiva.

Si bien la seguridad ciudadana es un objetivo prioritario, no debe sacrificarse el derecho fundamental a la privacidad. La captación y el tratamiento de imágenes mediante reconocimiento facial suponen una intromisión en la vida privada de los ciudadanos, especialmente cuando no existen garantías claras sobre el almacenamiento, acceso y eliminación de los datos recolectados. En este sentido, los especialistas consultados a través de las encuestas coincidieron en que el uso de esta tecnología debe estar sujeto a estrictas regulaciones que limiten la captación de datos biométricos a lo estrictamente necesario, garantizando transparencia y consentimiento informado. Asimismo, destacaron la necesidad de implementar altos estándares de seguridad, como la encriptación y la retención limitada de la información para prevenir posibles vulneraciones de derechos fundamentales.

En este contexto, la Directiva N° 01-2020-JUS/DGTAIPD establece disposiciones clave para garantizar la protección de los datos personales en sistemas de videovigilancia. En su numeral 6.6, referido al principio de calidad, se dispone que los datos recopilados solo deben conservarse durante el tiempo estrictamente necesario para cumplir con su finalidad. Asimismo, el numeral 6.13 determina que las imágenes y voces grabadas podrán almacenarse por un período de 30 días, extendiéndose hasta un máximo de 60 días, siendo responsabilidad del titular del banco de datos resguardar dicha información. En caso de que el material registrado contenga indicios delictivos, deberá ser remitido a la Policía Nacional del Perú o al Ministerio Público. Además, el numeral 6.8 enfatiza el respeto a los derechos fundamentales de los ciudadanos, señalando la responsabilidad del titular del banco de datos en la gestión adecuada de esta información sensible. Estas disposiciones buscan garantizar que la videovigilancia con inteligencia artificial se utilice de manera proporcional y bajo la normativa señalada en la Ley N°29733-Ley de Protección de datos personales.

Asimismo, la Opinión Consultiva N° 033-2022-JUS/DGTAIPD establece que las imágenes, videos o audios obtenidos a través de cámaras de videovigilancia instaladas en espacios de dominio público no pueden ser considerados de acceso público. Su divulgación sólo es legítima cuando se realiza en el marco de una investigación por la comisión de un presunto delito o falta, y únicamente pueden ser entregados a la Policía Nacional del Perú o al Ministerio Público, en estricta observancia de sus competencias. Cualquier uso distinto de esta información representaría una vulneración al derecho a la intimidad personal del titular de los datos.

Esta disposición refuerza lo establecido en el numeral 6.14 de la Directiva N° 01-2020-JUS/DGTAIPD, el cual enfatiza que los datos recopilados mediante videovigilancia deben ser tratados con confidencialidad y utilizados exclusivamente para los fines de seguridad previstos, evitando cualquier manejo indebido que pudiera afectar la privacidad de los ciudadanos.

El hecho de que las cámaras de videovigilancia se ubiquen en espacios públicos no implica que cualquier persona pueda acceder libremente a las imágenes, videos o audios captados. La Autoridad Nacional de Protección de Datos Personales ha señalado en diversas ocasiones, como en la Opinión Consultiva N° 55-2020-JUS/DGTAIPD, que esta información no constituye información pública, sino que está protegida por su naturaleza confidencial.

En concordancia con el Decreto Legislativo N° 1218 y la Ley de Transparencia y Acceso a la Información Pública, el acceso a estos datos sólo es legítimo cuando lo realizan autoridades competentes en el marco de sus funciones, como el personal municipal encargado de la seguridad ciudadana. En esta línea de ideas, la Opinión Consultiva 011-2023-JUS/DGTAIPD refuerza esta restricción al precisar que dichas grabaciones no son de acceso público si contienen datos personales de terceros, pudiendo incluso requerir una orden judicial para solicitar su acceso a ellas.

En conclusión, la incorporación de cámaras de videovigilancia con reconocimiento facial resulta una medida viable para fortalecer la seguridad ciudadana, especialmente en un contexto donde el país enfrenta un incremento alarmante de robos, asesinatos y secuestros. No obstante, su uso debe regirse por un riguroso análisis de proporcionalidad que garantice el respeto a los derechos fundamentales. Los especialistas consultados coincidieron en que esta tecnología solo es aceptable si se establecen límites claros, se minimiza el impacto en la privacidad y se implementan mecanismos de control adecuados para evitar abusos. De esta manera, se podría garantizar un equilibrio entre la necesidad de protección de la ciudadanía y la salvaguarda de la intimidad y otros derechos fundamentales.

A continuación, se procederá a analizar la segunda variable de este trabajo de investigación, centrada en la implementación de sistemas biométricos, como los sensores de reconocimiento dactilar, para el control laboral de los trabajadores. Este análisis evaluará el impacto de estas tecnologías en el ámbito laboral, considerando su uso como mecanismo de identificación y registro de asistencia.

En este contexto, resulta fundamental aplicar el test de proporcionalidad, examinando si estas medidas son idóneas, necesarias y proporcionales en relación con los derechos fundamentales involucrados. Entre los derechos que deben ser ponderados se encuentran el derecho a la intimidad y protección de los datos personales del trabajador frente al derecho del empleador a la seguridad y organización empresarial (derecho a la libertad de empresa, art. 59 de la Constitución Política del Perú), que podría verse afectado por un uso excesivo o desproporcionado de estos mecanismos de control.

1. Idoneidad: En cuanto a la idoneidad, el uso de sistemas biométricos, específicamente el reconocimiento dactilar, constituye un medio adecuado para garantizar la identificación precisa de los trabajadores en los centros de trabajo. Su implementación responde a la necesidad de prevenir fraudes o suplantaciones, asegurando un registro confiable de asistencia.

   En este sentido, la medida empleada se individualiza en la utilización de datos biométricos como mecanismo de control. No obstante, su aplicación implica una limitación al derecho a la privacidad y a la protección de datos personales, dado que se recolecta y almacena información sensible, lo que exige garantizar que su uso se ajuste a principios de proporcionalidad y seguridad en el tratamiento de los datos.

2. Necesidad: Respecto a la necesidad, es fundamental evaluar si existen métodos alternativos menos invasivos que permitan alcanzar el mismo objetivo de control laboral y seguridad en los centros de trabajo. Alternativas como el uso de tarjetas de identificación, códigos de acceso, credenciales personalizadas o el uso de cámaras de videovigilancia en zonas estratégicas pueden cumplir con la función de registrar la asistencia de los trabajadores sin recurrir a la recopilación de datos biométricos sensibles.

   Si bien el uso de sistemas biométricos, como el reconocimiento dactilar, garantiza un mayor nivel de precisión en la autenticación de los trabajadores, su implementación debe justificarse únicamente cuando no existan medios menos restrictivos que logren el mismo propósito. En este sentido, es importante diferenciar entre identificación y autenticación: la identificación permite reconocer a un individuo dentro de un grupo, mientras que la autenticación verifica con certeza su identidad.

Este matiz es clave para evaluar la necesidad del uso de datos biométricos en el control laboral, ya que si existen mecanismos que permitan autenticar a los trabajadores sin recurrir a la recopilación de información altamente sensible, su implementación podría no ser justificada.

En este contexto, el uso de cámaras de videovigilancia sin inteligencia artificial podría ser una opción intermedia que no recurre a la biometría, pero que, ubicadas en los accesos, permitirían verificar el acceso de los trabajadores de manera efectiva. De esta manera, se lograría un nivel adecuado de control sin comprometer de manera excesiva la privacidad de los trabajadores.

3. Proporcionalidad en sentido estricto: En este tercer paso del test de proporcionalidad, se exige un balance entre el beneficio obtenido y la afectación a los derechos fundamentales. En términos de medio, si bien los sistemas biométricos son idóneos para garantizar la identificación precisa de los trabajadores, también deben ser el menos lesivo posible para los derechos de estos.

   La recopilación de datos biométricos representa una intromisión significativa en la privacidad, ya que se trata de información única e irreemplazable, por lo que su uso debe limitarse estrictamente al registro de asistencia y contar con medidas de seguridad adecuadas, como encriptación, limitación en la retención de información y acceso restringido a los datos.

   En este sentido, la implementación de controles estrictos en el uso de datos biométricos no solo responde a una necesidad técnica de autenticación, sino que también implica una responsabilidad legal y ética. Es fundamental que su aplicación en el ámbito laboral se realice dentro de un marco regulatorio que garantice el respeto a la privacidad y los derechos de los trabajadores. La existencia de normas claras y mecanismos de supervisión adecuados permitiría minimizar los riesgos asociados al uso de información biométrica y asegurar que su implementación responda efectivamente a los principios de proporcionalidad.

Las entrevistas realizadas a expertos refuerzan la importancia de contar con una regulación específica sobre el uso de datos biométricos en el ámbito laboral, garantizando transparencia, límites claros y el consentimiento informado de los trabajadores. Fátima Toche Vega y Lyanee Pineda Abuhadba destacaron que el tratamiento de estos datos debe estar sujeto a un marco normativo detallado, asegurando que los trabajadores sean debidamente informados sobre el uso de su información y otorguen su consentimiento libre y expreso.

Por su parte, María Camargo Román y José Saul Casas Chuso señalaron que la implementación de estos sistemas debe responder a criterios de necesidad y proporcionalidad, evitando su uso indiscriminado y estableciendo medidas de seguridad adecuadas para prevenir accesos no autorizados. Asimismo, Carlos Jiménez Silva enfatizó que estos mecanismos deben ser herramientas de apoyo, sin sustituir la decisión final del empleador, siempre que se establezcan límites claros.

Desde la perspectiva del derecho, se debe ponderar el peso de los argumentos a favor de evitar la afectación. En este caso, la necesidad de una autenticación robusta en el control de asistencia es cuestionable, ya que no se trata de un sistema de acceso a información crítica o altamente sensible, sino únicamente de un registro horario de los trabajadores. Dado que existen métodos menos invasivos que pueden cumplir la misma función, se debe garantizar que la medida no imponga una restricción desproporcionada sobre el derecho a la privacidad.

Respecto al fin, es necesario evaluar el peso de los argumentos que justifican su implementación. Si bien el control de asistencia es un objetivo legítimo para garantizar la puntualidad y cumplimiento de las obligaciones laborales, este no debe prevalecer de manera absoluta sobre los derechos fundamentales de los trabajadores. En este sentido, la viabilidad del uso de sistemas biométricos dependerá de que se cumplan los principios de adecuación, necesidad y proporcionalidad, asegurando que no existan medios alternativos menos restrictivos que logren el mismo propósito.

En este contexto, resulta fundamental que los trabajadores sean debidamente informados sobre el propósito específico para el cual se recopilan sus datos biométricos. Si la recolección de huellas dactilares se justifica únicamente para el control de asistencia, debe existir certeza de que su uso no se extenderá a otros fines.

No obstante, no todas las empresas incluyen en sus contratos una cláusula específica sobre el tratamiento de datos sensibles y, cuando lo hacen, el trabajador suele aceptar estas condiciones por necesidad laboral, lo que limita la posibilidad de brindar un consentimiento realmente libre e informado, en contravención del principio de consentimiento.

Las entrevistas realizadas evidencian esta problemática: María Camargo Román, José Saul Casas Chuso y Lyanee Pineda Abuhadba señalaron que la falta de consentimiento adecuado agrava la asimetría de poder entre empleador y trabajador, dificultando la toma de decisiones informadas y generando riesgos para la privacidad. Por su parte, Fátima Toche Vega destacó que esta situación puede mitigarse mediante políticas claras de privacidad y un deber de información que garantice transparencia, alineándose con el principio de calidad, que exige que los datos sean veraces, pertinentes y tratados con medidas de seguridad adecuadas. En una línea similar, Carlos Jiménez Silva reconoció la asimetría existente, aunque consideró que puede ser justificada siempre que se establezcan límites adecuados y se informe de manera clara a los trabajadores, en concordancia con el principio de proporcionalidad, el cual exige que el tratamiento de los datos sea adecuado, relevante y no excesivo para la finalidad establecida.

En este sentido, el establecimiento de reglas precisas sobre la recolección y uso de datos biométricos resulta esencial para equilibrar la relación entre las partes y garantizar la protección de los derechos fundamentales, asegurando que las empresas cumplan con los principios esenciales que rigen el tratamiento de datos personales y evitando prácticas que vulneren la privacidad de los trabajadores.

Es por ello que, al comparar la regulación peruana con la de otros países como España, Brasil y México, se evidencia que el marco normativo en Perú sigue siendo poco claro y presenta vacíos legales significativos respecto al manejo de datos biométricos y el uso de inteligencia artificial en sistemas de videovigilancia. Mientras que en otras jurisdicciones existen normas específicas que regulan su uso tanto en el ámbito laboral como en el sector público, la legislación peruana aún carece de disposiciones detalladas que aborden los riesgos y desafíos que conlleva esta tecnología.

Para profundizar en este análisis, es útil revisar precedentes internacionales. Un ejemplo relevante es la Sentencia 190/2023 del Juzgado de lo Social N° 2 de Alicante (España), donde se determinó que el uso del reconocimiento facial para el control de asistencia laboral vulneraba el derecho a la intimidad del trabajador.

El tribunal concluyó que la empresa había adoptado un método excesivamente intrusivo, sin realizar un análisis previo de impacto ni contar con un consentimiento específico. Además, subrayó que existían alternativas menos invasivas, como tarjetas de acceso, que habrían cumplido el mismo objetivo sin comprometer derechos fundamentales. Este precedente refuerza la exigencia de que, antes de implementar sistemas biométricos para el control laboral, se debe someter la medida a un riguroso test de proporcionalidad.

Otro aspecto relevante identificado en el análisis es la ausencia de mecanismos eficaces para la fiscalización y sanción ante el incumplimiento de la normativa de protección de datos personales. Casos como la sanción impuesta al BCP por la recolección y almacenamiento indebido de datos biométricos evidencian la necesidad de reforzar la supervisión de las prácticas empresariales en este ámbito.

En conclusión, el uso de la huella dactilar como método de control laboral no resulta proporcional ni estrictamente necesario, ya que existen alternativas menos intrusivas que pueden cumplir el mismo propósito sin comprometer en exceso la privacidad de los trabajadores. En este sentido, las cámaras de videovigilancia convencionales representan una opción intermedia que permite verificar la identidad sin recurrir a la recopilación de datos biométricos sensibles, reduciendo así los riesgos asociados a su almacenamiento y posible uso indebido.

Si bien la biometría puede ofrecer beneficios en términos de seguridad y eficiencia, su implementación en el ámbito laboral debe estar supeditada a un marco normativo claro que garantice la transparencia en su uso y evite vulneraciones a los derechos fundamentales. La inexistencia de una regulación específica en el Perú sobre la recopilación y tratamiento de datos biométricos genera un escenario de incertidumbre, en el que los trabajadores pueden verse obligados a aceptar el uso de estas tecnologías sin un consentimiento realmente libre e informado.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

1. El reconocimiento biométrico en el Perú es una herramienta relativamente nueva en el país, por este motivo las normas, leyes y el marco jurídico en general referente a este tema puede ser insuficiente en función de la protección de datos personales de los ciudadanos, donde, actualmente el uso de esta tecnología es más común en el sector laboral, ya que muchas empresas e instituciones públicas están implementando sistemas de control de asistencia y salida de sus trabajadores mediante biometría pero a su vez este tipo de sistemas están siendo cuestionados sobre la posibilidad, de que al implementarlos, se esté vulnerando la privacidad de las personas.

2. La implementación de cámaras de videovigilancia con tecnología de reconocimiento facial se presenta como una opción viable para mejorar la seguridad pública, especialmente en un contexto de creciente violencia, como robos, homicidios y secuestros. Sin embargo, su utilización debe estar sujeta a un análisis riguroso de proporcionalidad, asegurando que se respeten los derechos fundamentales de las personas. De esta forma, se podría lograr un balance adecuado entre la necesidad de protección ciudadana y la defensa de la privacidad y otros derechos fundamentales.

3. Al comparar la regulación peruana con países como España, se puede evidenciar que aún nos falta mucho por avanzar en cuanto a la protección de los datos personales. En otras jurisdicciones existen leyes específicas que regulan el uso de datos biométricos tanto en el ámbito laboral como en la videovigilancia ciudadana.

4. Existen alternativas menos invasivas que podrían cumplir el mismo objetivo que la biometría sin comprometer derechos fundamentales. En algunos casos, el uso de la biometría ha sido considerado desproporcionado por no haber realizado un análisis de impacto adecuado.

6.2. Recomendaciones

1. Se debe garantizar que los trabajadores brinden su consentimiento informado de manera libre, informada y expresa antes de la recopilación de sus datos biométricos. Esto mitigaría la asimetría de información y evitaría las prácticas abusivas.

2. La implementación de IA en cámaras de vigilancia es una herramienta poderosa para mejorar la seguridad, pero su uso debe ser estrictamente regulado para evitar sesgos, errores y vulneraciones de la privacidad. La regulación debe garantizar la equidad, la protección de datos personales, la responsabilidad, y el respeto por los derechos fundamentales. Esto incluye establecer controles y auditorías regulares, limitar el uso de los sistemas a finalidades específicas, y asegurar que los datos sean protegidos adecuadamente.

3. Antes de implementar los sistemas biométricos, se debe considerar la proporcionalidad debida para determinar si existen métodos menos invasivos que puedan cumplir el mismo objetivo ya que existen alternativas como tarjetas de acceso, códigos personales o cámaras de vigilancia tradicionales que funcionan sin incorporar sistemas biométricos podrían ser suficientes en muchos casos.

BIBLIOGRAFÍA

Libros

Domínguez, Ana Garcia. *Tratamiento de Datos Personales y Derechos Fundamentales*.Madrid: Editorial DYKINSON,2024.

Diaz, Vanessa. *El Ejercicio de los Derechos ante el Flujo de Información Biométrica.* México: Editorial UNAM, 2016.

Mender Bini, Susan. *Sistemas Biométricos.* Argentina: Editorial Eldial, 2024.

Capítulos de libros

Celis Quintal, Marcos Alejandro. "La protección de la intimidad como derecho fundamental de los Mexicanos, 71-108". En *Protección de la persona y derechos fundamentales*. México: UNAM, 2006.

César Puntriano, "La videovigilancia en el ámbito laboral", en *El Derecho del Trabajo y la Seguridad Social en época de cambios* (Lima: Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social, 2020), 728.

Morales Godo, Juan. "Derecho al honor, buena reputación, intimidad personal y familiar, voz e imagen, 275-285". En *La Constitución comentada*. Lima: Gaceta jurídica,2005.

Morales Godo, Juan. "El derecho a la intimidad y el conflicto con el derecho a la información, 119-137". En *La Constitución comentada*. Lima: Gaceta jurídica, 2005.

Peschard, Jacqueline. "Cien años del derecho a la privacidad en la Constitución, 361-378". En *Cien ensayos para el centenario. Constitución Política de los Estados Unidos Mexicanos.* México: Instituto de Investigaciones Jurídicas, 2017.

Libros electrónicos

Autoridad Nacional de Protección de Datos Personales. *El Derecho Fundamental a la Protección de Datos Personales: Guía para el Ciudadano*. Lima: Ministerio de Justicia y Derechos Humanos, 2013. https://cdn.www.gob.pe/uploads/document/file/1401558/El%20derecho%20fundamental%20a%20la%20protecci%C3%B3n%20de%20datos%20personales.pdf.

Artículo de revistas académicas impresas

Angles Yanqui, Gerard Henry. "TikTok:La ineficacia del derecho a la intimidad en la era digital en tiempos de Covid-19 y el "famoso" derecho al olvido en Perú". *Revista de Derecho* 5, no.1 (2020): 194-201.

Jaccottet Freitas, Gustavo. "Privacidad, intimidad: Un debate sobre los alcances de las limitaciones a los Derechos Fundamentales y la visión de la libertad de expresión ante la novela 1984 de George Orwell". *Revista Latinoamericana de Derechos Humanos*, no.25 (2014): 79-94.

Mubarak Aguad, Laisha. "El internet, el Bigdata y el tratamiento de datos personales". *Advocatus*, no.36 (2017): 205-223.

Moreno Jorge, María, Jorge Ivan Porras Aragón y Carlos Marco Céspedes Gonzales, "Uso de herramientas tecnológicas para la prevención del crimen". *Revista Académica de la Escuela de Posgrado de la Policía Nacional del Perú 3*, no.1 (2023): 34-43.

Negro Pavón, Dalmacio."John Stuart Mill: el liberalismo como ideología". *Revista de estudios políticos* 159, no.1 (1968): 121-145.

Artículos en revistas académicas

Alvarado, Francisco Javier. "La gestión de la seguridad de la información en el Régimen Peruano de Protección de Datos Personales". *Foro Jurídico*, no 15 (2016): 26-41. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19833.

Aragüez Valenzuela, Lucía. "Debates emergentes en materia laboral y de privacidad: Sistemas de videovigilancia, algoritmos digitales e identificación biométrica de la persona trabajadora". *THEMIS Revista De Derecho*, no.79 (2021): 451-466. https://doi.org/10.18800/themis.202101.026.

Blume Moore, Iván. "Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales". *THEMIS Revista De Derecho*, no. 79 (2021): 435-449. https://doi.org/10.18800/themis.202101.025

Blume Moore, Iván. "El derecho fundamental a la protección de datos personales en el entorno laboral". Laborem, no. 24 (2021): 265-287. https://www.spdtss.org.pe/wp-content/uploads/2021/09/Laborem24-12-1. pdf.

Barona Vilar, Silvia. "Tecnologia biometrica y datos biométricos.Bondades y peligros. No todo vale". *Actualidad Jurídica Iberoamericana*, no. 21 (2024): 300-330, https://revista-aji.com/wp-content/uploads/2024/07/AJI21_Art11.pdf

Chilano, María Belén. "Intimidad en la era digital: análisis jurídico y enfoque juvenil sobre percepciones y prácticas". *Derecom. Derecho de la Comunicación y de las Nuevas Tecnologías*, no.35 (2024): 4256. https://revistas.ucm.es/index.php/DERE/article/view/98693

Eguiguren Praeli, Francisco José. "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú". *THEMIS Revista De Derecho*, no. 67 (2015): 131-140. https://revistas.pucp.edu.pe/index.php/themis/article/view/14462

Eguiguren Praeli, Francisco. "La libertad de información y su relación con los derechos a la intimidad y al honor en el caso Peruano". *IUS ET VERITAS* 10, no. 20 (2000): 51-75. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15924.

Eugenio Dotti, Jorge. "Observaciones sobre Kant y el Liberalismo". *Araucaria* 7, no.13 (2005): 4-17. https://revistascientificas.us.es/index.php/araucaria/article/view/1088.

López Torres, Jonathan. “Antecedentes internacionales en materia de privacidad y protección de datos personales”. *Universidad EAFIT Revistas Académicas* 5, no. 2 (2014): 103-117. https://publicaciones.eafit.edu.co/index.php/ejil/article/view/2849/2616

Martínez de Pisón Cavero, José María. “El Derecho a la Intimidad: De la configuración inicial a los últimos desarrollos de la jurisprudencia constitucional”. *Anuario de filosofía del Derecho*, no. 32 (2016): 410-430. https://revistas.mjusticia.gob.es/index.php/AFD/article/view/2301.

Maqueo Ramírez, María Solange, Jimena Moreno Gonzáles y Miguel Recio Gayo. "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario". *Revista de Derecho XXX*, no. 1 (2017): 77-96, https://www.redalyc.org/articulo.oa?id=173752279004

Murillo Chávez, Javier André. “Brace yourselves! La videovigilancia ya viene:situación de la videovigilancia en el ordenamiento jurídico peruano”. *Derecho PUCP,* no.83 (2019): 133-178. https://doi.org/10.18800/derechopucp.201902.005.

Olivos Celis, Milagros Katherine. “La protección de la privacidad como objeto de tutela en el ordenamiento jurídico Peruano”. *IUS: Revista de Investigación de la Facultad de Derecho* 8, no.1 (2019): 47-67. https://doi.org/10.35383/ius.v1i1.38.

Polo Roca, Andoni.“Privacidad, intimidad y protección de datos: Una mirada Estadounidense y europea”. *Derechos y libertades: Revista de Filosofía del Derecho y Derechos Humanos*, no.47 (2022): 308 -338. https://doi.org/10.20318/dyl.2022.6884.

Velasco Pérez, Zuleymi. “Derecho penal y protección de datos personales”. *Llapanchikpaq: Justicia 6,* no.9 (2024): 133-160. https://revistas.pj.gob.pe/revista/index.php/lj/article/view/1042/1449

Vásquez Rodríguez, Raúl. “El consentimiento para tratamiento de datos personales de salud en tiempos del COVID-19”. *YachaQ Revista De Derecho*, no. 11 (2020): 145-164. https://doi.org/10.51343/yq.vi11.366.

Artículo en un periodo impreso o digital

Antelo, Gabriel. “De las huellas dactilares a los datos biométricos”. *El Peruano*, 6 de diciembre de 2024. https://elperuano.pe/noticia/259487-de-las-huellas-dactilares-a-los-datos-biometricos

Campos Barranzuela, Edhin. “Cámaras de vigilancia en el Perú”. *Lp Pasión por el Derecho*, 9 de julio de 2019. https://lpderecho.pe/camaras-vigilancia-peru-edhin-campos-barranzuela/

Gestión, “Interbank: Fiscalía en ciberdelincuencia inició diligencias sobre presunto hackeo”, *Gestión,* 30 de octubre de 2024*,* *https://gestion.pe/economia/interbank-hackeo-fiscalia-en-ciberdelincuencia-inicio-diligencias-sobre-presunto-hackeo-indecopi-datos-de-usuarios-noticia/?utm_source=chatgpt.com*

Luis Miguel Martínez Anzures, “Los datos biométricos en México: La cultura de la desconfianza” *El Heraldo de México*, 23 de abril de 2021. https://heraldodemexico.com.mx/opinion/2021/4/23/los-datos-biometricos-en-mexico-la-cultura-de-la-desconfianza-287722.html

Mamani Gutiérrez, Elani Yahaira. “Reglamento de la ley de protección de datos personales [Decreto Supremo 016-2024-JUS]. Lp Pasión por el Derecho. 30 de noviembre de 2024. https://lpderecho.pe/reglamento-ley-proteccion-datos-personales-decreto-supremo-016-2024-jus/

Artículos en espacios web académicos

Boletín semanal SBS, “Servicios Financieros digitales: el uso de la biometría para proteger las operaciones financieras”, Superintendencia de Banca, Seguros y AFP (SBS), 6 de marzo de 2025, https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/2293

Editorial Leto.“Uso de datos biométricos en la oficina”. RH en las empresas. 26 de septiembre de 2024. https://rhenlasempresas.com/2024/09/26/datos-biometrico/

Elizario de Lima, Carlos; Gomes, Lucas. “Autoridad Nacional de Protección de Datos de Brasil: estructuración e iniciativas”. iapp (International Association of Privacy Professionals). 8 de septiembre de 2021. https://iapp.org/news/a/autoridad-nacional-de-proteccion-de-datos-de-brasil-estructuracion-e-iniciativas/

Guerrero, Carlos y Martín Borgioli. “Identidad Biométrica en Perú”. Hiperderecho. 6 de junio de 2018. https://hiperderecho.org/wp-content/uploads/2018/06/identidad_biometrica_peru_2018.pdf

Organización de las Naciones Unidas. "Declaración Universal de Derechos Humanos." Naciones Unidas. 10 de diciembre de 1948. https://www.un.org/es/about-us/universal-declaration-of-human-rights.

Puntriano Rosas, Cesar Alfredo. “La videovigilancia en el ámbito laboral”, IX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social. 19 de febrero.https://www.spdtss.org.pe/wp-content/uploads/2021/10/IX-Congreso-Nacional-full-719-747.pdf

Documento institucional en línea

Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP). 2023. *Saber es tu poder: Derecho al acceso a la información pública*. Lima: Ministerio de Justicia y Derechos Humanos. https://www.gob.pe/institucion/antaip/informes-publicaciones/3455744-saber-es-tu-poder-derecho-al-acceso-a-la-informacion-publica.

Defensoría del Pueblo. “*Manual de Protección de Datos Personales”*. Lima: Defensoría del Pueblo, 2019. https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf.

Defensoría del Pueblo, *“Manual de excepciones al acceso a la información pública”*. Lima: Defensoría del Pueblo, 2016. https://www.defensoria.gob.pe/wp-content/uploads/2018/08/Manual-excepciones-al-acceso-info-publica-2016.pdf.

Ministerio de Justicia y Derechos Humanos, "MINJUSDH sanciona a entidad financiera por inadecuado tratamiento de datos personales biométricos solicitados a sus usuarios", Gob.pe, 6 de enero de 2025, https://www.gob.pe/institucion/minjus/noticias/1086705-minjusdh-sanciona-a-entidad-financiera-por-inadecuado-tratamiento-de-datos-personales-biometricos-solicitados-a-sus-usuarios

Tesis y trabajos de grado

Jara Villacís, Mónica. "El derecho a la intimidad y la presentación de correos electrónicos como prueba". Tesis para optar el grado de Especialista en Derecho Constitucional, 2013.

Macutela Lavilla, Nataly. "Tratamiento de datos personales sensibles en Perú en el contexto de Covid-19". Tesis para optar el título de segunda especialidad en Derecho Administrativo, Pontificia Universidad Católica del Perú, 2020.

Entrada o comentario a un blog

Loza, María; Monreal, Patricio. "Biometría en el Entorno Laboral", *Govertis (blog),* 12 de diciembre de 2023. https://www.govertis.com/biometria-en-el-entorno-laboral

Normas citadas

Directiva N° 01-2020-JUS/DGTAI-PD, de 16 de enero de 2020, Tratamiento de Datos Personales mediante Sistemas de Videovigilancia. (Lima, 17 de marzo de 2020).

Dirección de Protección de Datos Personales, Resolución Directoral N° 2629-2022-JUS/DGTAIPD-DPDP, de 14 de julio de 2022.

Ley 29733-2011, de 3 de Julio, Ley de Protección de Datos Personales (Lima, 3 de julio de 2011).

Resolución Directoral N°2271-2024-JUS/DGTAIPD-DPDP., EXP.N° 122-2023-JUS/DGTAIPD-PAS, 1 de julio de 2024.

Resolución Directoral N°110-2024-JUS/DGTAIPD, EXP.N°122-2023-JUS/DGTAIPD-PAS, 27 de diciembre de 2024.

Jurisprudencia citada

Corte Suprema de Justicia de la República, Sala Penal Permanente R. N. N.° 300-2021, de 10 de Noviembre de 2021.

Ministerio de Justicia y Derechos Humanos, Opinión consultiva N° 032-2021-JUS/DGTAIPD, de 17 de agosto de 2021.

Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 033-2022-JUS/DGTAIPD, de 2 de septiembre de 2022.

Ministerio de Justicia y Derechos Humanos. Opinión Consultiva 011-2023-JUS/DGTAIPD, de 21 de marzo de 2023.

Ministerio de Justicia y Derechos Humanos. Opinión Consultiva N° 011-2023-JUS/DGTAIPD, de 21 de marzo de 2023.

Sentencia del Tribunal Constitucional. EXP N°579-2008-PA/TC.

Tribunal Constitucional, Exp. N.º 6712-2005-HC/TC, 17 de octubre de 2005.

Tribunal Constitucional. EXP.N° 02208-2017-PA/TC, de 25 de septiembre de 2020.

Tribunal Constitucional del Perú, Sentencia N° 166/2021, de 2 de febrero de 2021.

Derecho comparado

Juzgado de lo Social N° 2 de Alicante. Sentencia N° 190/2023, de 15 de septiembre de 2023.

Lei Nº 12.527/2011 - LAI, de 18 de noviembre, Lei de acesso a informaçõ pública. (Brasil, 16 de mayo de 2012)

Ley N° 13.709/2018, de 14 de agosto, Lei Geral de Proteção de Dados. (Brasil, 15 de agosto de 2020).

Ley Orgánica 3/2018, de 5 de diciembre, Ley de Protección de Datos Personales y Garantía de los derechos digitales. (Madrid, 6 de diciembre de 2018).

Reglamento (UE) 2016/679, de 27 de abril, Reglamento General de Protección de Datos. (Unión Europea, 5 de mayo de 2016)

Tribunal de Justiça do Estado de São Paulo (TJSP) 37ª Vara Cível do Foro Central Cível de São Paulo. N° 1090663-42.2018.8.26.0100, de 7 de mayo de 2021.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados/2017 - de 26 de enero, LGPDPPSO. (Ciudad de México, 26 de enero de 2017)

Ley Federal de Protección de Datos Personales en Posesión de los Particulares/2010 - de 5 de julio, LFPDPPP. (Ciudad de México, 5 de julio de 2010)

Tribunal Pleno de la Suprema Corte de Justicia de la Nación LXIV Legislatura Ciudad de México. N° 82/2021 y N° 82/2021, de 25 de abril de 2021.

ANEXOS

Anexo N°1: Matriz de Consistencia

	GENERAL	ESPECÍFICO 1	ESPECÍFICO 2
PROBLEMÁTICA	¿De qué manera el uso del reconocimiento biométrico afecta el derecho a la protección de datos personales en el ámbito de la videovigilancia ciudadana y el control laboral? ¿Las instituciones están tomando medidas suficientes para garantizar la autodeterminación informativa de los ciudadanos y trabajadores?	¿Cuáles son los principales riesgos que el reconocimiento biométrico plantea para la protección de datos personales y la autodeterminación informativa en la vigilancia ciudadana y el control laboral?	¿Cómo se ha abordado en otros países la regulación sobre la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral? ¿Qué medidas han adoptado para garantizar la protección de los datos personales y la autodeterminación informativa de los ciudadanos?
OBJETIVOS	Determinar cuales son las consecuencias jurídicas derivadas del uso del reconocimiento biométrico en la videovigilancia ciudadana y el control laboral, con el propósito de evaluar su impacto en la protección de datos personales y la garantía del derecho a la autodeterminación informativa.	Determinar los principales riesgos jurídicos que genera la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral en el Perú, evaluando su impacto en la protección de datos personales y en el derecho a la autodeterminación informativa.	Evaluar de qué manera han abordado otros países la regulación sobre la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral sobre la protección de datos personales.
HIPÓTESIS	El uso del reconocimiento biométrico en la vigilancia ciudadana y el control laboral supone una vulneración al derecho a la protección de datos personales, especialmente cuando las medidas adoptadas por las entidades no garantizan de manera efectiva la autodeterminación informativa de los individuos.	La implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral genera riesgos para la protección de datos personales. Si bien en el ámbito de la videovigilancia existen medidas de protección, en el control laboral la falta de una regulación específica podría derivar en consecuencias jurídicas como la vulneración del derecho a la privacidad y la autodeterminación informativa.	En otros países, como en España, la regulación sobre la implementación del reconocimiento biométrico en la vigilancia ciudadana y el control laboral establecen límites estrictos para el tratamiento de datos biométricos, exigiendo principios como la proporcionalidad y la minimización de datos.

Anexo N°2: Transcripción de las Entrevistas

ENTREVISTA 1:

Fecha: 25 de febrero del 2025

Hora: 9:00 p.m

Lugar: Lima, Perú

Entrevistado: Carlos Jiménez Silva - Abogado especializado en Derecho del Trabajo y Seguridad Social

1. ¿Está familiarizado con la Ley N° 29733, ley que protege los datos personales? ¿Cree que debería existir una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos?

   Desde el punto de vista laboral, a partir del reglamento que ha sacado la Unión Europea, que todavía no hay en nuestro país, lo que tiene que haber es que las decisiones que tome el empleador sobre la base de su poder de dirección, que deriva de la libertad de empresa, que están aterrizadas en el artículo 59 de la Constitución y a nivel infraconstitucional en el artículo 9 del Decreto Supremo 003-97 TR, pueden servir de base, antes de tomar una decisión de promoción, de suspensión, de amonestación o hasta de vinculación, la inteligencia artificial, que lo que tiene que tomar la decisión es el empleador. Ese es un límite que tiene que ponerse.

   El segundo límite está referido a que los trabajadores sean informados directamente o a través de la organización sindical de quién ha hecho la programación y para qué fines ha hecho la programación. En tercer lugar, tiene que regularse la protección de datos personales del trabajador. Si el empleador, por razón del servicio, ha tomado ciertos exámenes médicos del trabajador, esa información no puede ser revelada por el médico ocupacional o por la tercera empresa a cargo de los exámenes médicos, inclusive al empleador, solamente al trabajador. ¿Por qué? Porque está protegida con la protección de datos personales, a menos que se trate de una enfermedad de infecto contagioso, por ejemplo, que esté vinculada, por ejemplo, a la

tuberculosis, que hay una etapa que se compacta a través del esputo. Por otro lado, algunos medios electrónicos que se utilizan para el ejercicio del poder de dirección del empleador, han sido fuertemente cuestionados, como por ejemplo, el uso de lectura del iris del ojo, porque puede determinar determinadas enfermedades del trabajador o puede discriminar a determinadas categorías de trabajadores que tengan ciertas enfermedades o dolencias que a veces no están justificadas. Para entrar en ciertos sitios de la empresa podría entonces pedir el iris del ojo.

Entonces la inteligencia artificial es buena, pero bajo ciertos límites, y esos límites tienen que estar regulados, tienen que especificarse por parte del empresario al trabajador cuál es el objetivo de esa optimización de la inteligencia artificial y cómo ha sido programada. Porque también podemos decir que puede haber discriminaciones al momento del ascenso, al momento de la contratación o al momento de la vinculación. Podría, por ejemplo, por razones no objetivas, perjudicar a una determinada categoría de trabajadores que están sindicalizados, porque así es programado la inteligencia artificial al momento de tomar decisiones o promociones o a determinado sexo de trabajadores. Por eso está bien la inteligencia artificial como una ayuda, pero no la que tome decisiones. Y por otro lado, que se informe al trabajador sobre los alcances y objetivos de esta herramienta.

La inteligencia artificial debe regularse en cuanto al porqué de la utilización en las relaciones de trabajo dentro de la empresa, cuál es el objetivo, cuál es el fin y la última palabra la tiene que tomar el empleador, por lo que es la base del principio de razonabilidad y proporcionalidad. Y el uso de la inteligencia artificial puede tener varios usos, al momento del acceso al empleo, al momento de la promoción, al otorgamiento de beneficios y al momento de la vinculación, así como también al movimiento de traslados dentro de la empresa y también, pues, al tomar ciertos exámenes médicos que se requieran para el ejercicio de las labores contratadas. En el caso específico del país, existe una directiva del Ministerio de Justicia sobre el uso de las cámaras de video, que deben estar puestas en una forma no escondida, sino que sea un lugar visible y que no sea un sitio de descanso donde uno toma sus alimentos, o las camarines, o las duchas. Y se tiene que informar al trabajador.

2. ¿Existe asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos? ¿Considera que esta falta de transparencia limita la posibilidad de tomar decisiones informadas sobre su uso?

   El derecho al secreto de las comunicaciones y el derecho a la intimidad es un derecho garantizado en la Constitución para cualquier ciudadano. Es un derecho en específico que se convierte en específico desde una relación de trabajo.

   El empleador, sobre la base de su poder de dirección que deriva de la libertad de empresa, puede utilizar una gobernanza sobre las relaciones de trabajo. Pero esto tiene ciertos límites y los límites tienen que ver con el secreto de las comunicaciones que supone que no puede ingresar al correo electrónico el trabajador para saber qué información está utilizando y también el secreto de las comunicaciones o bueno, el secreto de la imagen, por ejemplo. Ese es otro derecho en específico.

   Por ejemplo, yo no podría utilizar por fines propagandísticos la imagen del trabajador ni tampoco prohibir que pueda emitir opinión. El trabajador puede emitir opinión sobre lo que le parece la marcha de la empresa y no podría ser sancionado salvo que impugne o difame al empleador o a su representante. Pero la libertad de opinión está garantizada en la Constitución.

   Entonces el empleador, si bien es cierto, bajo su facultad directriz puede reglamentar, fiscalizar y sancionar, estos tienen ciertos límites que son los derechos de los trabajadores. Entonces estamos frente a dos derechos. Por un lado la libertad de empresa que está garantizada en el artículo 2.59 de la Constitución y por otro lado el secreto de las comunicaciones que está garantizado en el artículo 2.10 de la Constitución. ¿Qué derecho debe primar? Pues ahí aplicamos el test de proporcionalidad. ¿Cuál es el derecho más idóneo, más necesario y más proporcional? Es válido que el empleador pueda utilizar los medios tecnológicos para marcar el ingreso y salida del trabajador, tanto en la empresa como en la salida, porque está dentro del principio de la razonabilidad y no vulnera ningún derecho en específico del trabajador. No, eso está regulado en la norma. Entonces, si va a utilizar los datos biométricos

como la huella digital para ingresar es una medida válida. Lo que no sería correcto sería, por ejemplo, y se puede cuestionar, es que se utilice la lectura del IRIS de ojo para ingresar a determinadas áreas que puede determinar que el trabajador tenga cierto tipo de enfermedades y eso podría originar que sea determinado por tener cierto tipo de enfermedades que no son determinantes para la contratación.

3. Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo considera que una violación de seguridad podría afectar la privacidad de los trabajadores en el ámbito laboral?

   Existe un derecho constitucional que es el secreto de la información, está garantizado en los dos imprecisos medidas de la Constitución, el derecho a la intimidad del trabajador. La intimidad tiene que ver con el aspecto personal intrínseco del trabajador, por ejemplo, determinar si el trabajador tiene algún tipo de enfermedad que nada más le corresponde a él saberla y no habría que comunicar ni al empleador ni a los otros trabajadores. Ese sería un caso.

   Pero por otro lado, estamos viendo que a veces el empleador no respeta eso y salta la información. Lo que ha pasado ahora, por ejemplo, con Shakira, ha salido del ámbito de la clínica del grado, aparentemente fue por un mal elemento, un mal trabajador, una información de la vida personal de esta cantante y ha sido multada en esta clínica, como he entendido, por indecopi, por sacar información. Así como esa información puede ser de terceros, también puede ser de los pocos trabajadores. No se justifica. ¿Y en qué caso se justificaría que se comunique por el médico ocupacional de la empresa los resultados de un examen médico al trabajador? Por ejemplo, si el trabajador tiene tuberculosis y está en la etapa del contagio, ahí el trabajador no puede asistir a trabajar y es importante que se comunique al empleador a través de su representante para que el trabajador no vaya a trabajar, porque está ahí por medio la comunidad, todos los demás trabajadores que pueden verse afectados. Ahí sí se aplica el principio de la personalidad de la persona. Entonces hay que ver cada caso, Ahora la pregunta sería, ¿y el trabajador podría aceptar que sus datos sean revisados por la empresa y eventualmente comunicados a los demás trabajadores? ¿O se aplica el principio de

irrenunciabilidad de derechos? Considero que el trabajador podría aceptar, porque él es integrante de esos derechos, que estos se puedan conocer por el empresario y eventualmente comunicar a terceras personas. Sin embargo, debo decir que hay parte de la opinión que dice que eso se podría dar en la medida que se trate de datos no sensibles, o sea, vinculados a la prestación del servicio, pero algo que no tenga nada que ver con la prestación del servicio. Por ejemplo, si la trabajadora puede tener o no familia, no deberían casos. Entonces ahí sí podría invocar que estaría renunciando a un derecho al momento de firmar ese acuerdo, porque si no, no contratan al trabajador.

4. ¿Qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas?¿Cuál es su opinión sobre el uso de la inteligencia artificial en las cámaras de videovigilancia en el Perú y su impacto en la privacidad de los ciudadanos?

   Bueno, creo que el uso de los datos biométricos se justifica siempre y cuando se le comunique al trabajador el objetivo de su uso, para qué se utilizan esos datos biométricos y que esté vinculado a la prestación del servicio. Si hay una razonabilidad y una proporcionalidad en la utilización de los mismos, y se le explica al trabajador por qué se utilizan los mismos recorridos. Las cámaras de videovigilancia ya están reguladas. Es una directiva del Ministerio de Justicia. La videovigilancia tiene que estar en un lugar visible, no oculto. Tiene que estar en donde se presta la prestación del servicio, que puede ser cuando el trabajador está en contacto con terceras personas o dentro del propio centro de trabajo sin contacto con terceras personas pero no puede estar en sitios de esparcimiento, de descanso, de recreo, en las duchas, en las balerinas.

   El objetivo de las cámaras de videovigilancia es básicamente proteger los bienes del empresario. En segundo lugar, evitar infortunios laborales, accidentes de trabajo o accidentes de enfermedades profesionales de cara al principio de prevención del empleador, y, en tercer lugar, mejorar la productividad de la empresa. Entonces, la inteligencia artificial podría ayudar si está encaminada en ese sentido y si se informa previamente a los trabajadores de por qué es usado. Y que el que tome la decisión en última instancia, sea el empresario. Porque la inteligencia artificial ve las cosas en

forma fría, pero no tiene en consideración ciertos aspectos de carácter personal que podrían de alguna manera variar la decisión que se toma.

No vulneraría ningún derecho de los ciudadanos porque hay un fin superior siempre y cuando se explique que eso o un aviso que hay una cámara de videovigilancia con reconocimiento facial no puede ser algo justo, ¿no? Porque eso de alguna manera garantiza la seguridad de los bienes del empresario, del negocio, evitar asaltos, evitar robos y también, ¿por qué no?, infortunios laborales. Esta persona no está capacitada y se ha identificado que no está capacitada para entrar a determinadas áreas de la empresa donde se manejan productos químicos o biológicos. Entonces, se identifica con las cámaras y automáticamente se la retira por el personal de seguridad. Entonces, sí, sí es importante utilizar la tecnología, pero siempre utilizando esta proporcionalidad y racionalidad, ¿no? Y que esté vinculada a la prestación del servicio. Es buena la inteligencia artificial, pero con ciertos límites.

ENTREVISTA 2:

Fecha: 3 de Marzo del 2025

Hora: 4:00 p.m

Lugar: Lima, Perú

Entrevistado: Fátima Toche Vega - Abogada especializada en Derecho Digital y Nuevas Tecnologías, con formación en la Pontificia Universidad Católica del Perú.

1. ¿Está familiarizado con la Ley N° 29733, ley que protege los datos personales? ¿Cree que debería existir una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos?

   Sí, completamente. Yo creo que valía la pena en el reglamento, en el nuevo reglamento de la ley, hacer una indicación particular sobre los datos biométricos, ¿no? Dar un detalle un poco mayor respecto a la utilización de datos biométricos. No obstante, a cualquier captación de datos, ya sean personales o sensibles, se tiene que cumplir con todos los principios rectores que están señalados en la ley, ¿no? Es una forma más de tratamiento y merece el rigor del tratamiento de cualquier dato personal, pero yo creo que debido al

uso que tiene la biometría para temas importantes como temas de seguridad ciudadana, temas de autenticación de identidad, sí valía la pena darle un tratamiento especial.

2. ¿Existe asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos? ¿Considera que esta falta de transparencia limita la posibilidad de tomar decisiones informadas sobre su uso?

   Sí, pero recuerda que la asimetría siempre, digamos, así como pasa en protección al consumidor, siempre va a haber algún tipo de asimetría entre el ciudadano y la empresa o entidad que capta el dato, porque es únicamente a ciencia cierta sabe para qué se van a utilizar los datos la empresa o la entidad que los capta.

   Entonces, siempre va a haber cierto nivel de asimetría, ok? Pero esa asimetría se puede, de alguna manera, mitigar con el deber de información. ¿Y dónde se canaliza ese deber de información? En la política de privacidad, en los documentos informativos que el ciudadano debe poder leer y acceder antes de dar el consentimiento. Entonces, obviamente cuando no se capta el consentimiento del ciudadano hay el peor caso de asimetría y cuando el ciudadano es informado parcialmente hay un gran nivel de asimetría también, pero podría haber una situación ideal en la que las empresas o entidades públicas informen correctamente y obviamente estén dentro de algún marco de legitimación para la captación, porque ese es el primer paso que hay que analizar, y que pueda haber un equilibrio más o menos de entre el poder del ciudadano al conocer para qué fines están captando sus datos y el de la empresa para utilizarlos.

3. Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo considera que una violación de seguridad podría afectar la privacidad de los trabajadores en el ámbito laboral?

   Yo creo que lo principal ahí, en esa forma de captación para el fin de, por ejemplo, de marcación de entrada y salida de un trabajador, lo principal ahí es el análisis de proporcionalidad, es decir, captar y tratar un dato sensible como

es la biometría, es proporcional para un control de entrada que tal vez tiene 20, 30 formas distintas en el que se puede hacer y que es menos invasivo, lo primero ahí yo creo que sería la proporcionalidad, ¿no? Y recuerda que la norma peruana dice que sólo se puede crear un banco de datos sensibles cuando esto está íntimamente ligado a la función o giro del negocio del titular del banco, ¿no? O al objetivo de ese banco de datos, ¿no? Entonces incluso si lo vemos desde el punto de vista también constitucional y con ponderación de derechos, ahí hay un problema, ¿no? Y segundo, ¿cuáles son los potenciales riesgos? Que hay alguna brecha de seguridad que exponga esos datos y con los datos biométricos tú sabes que se puede acceder hoy por hoy hasta préstamos bancarios, acceder a hacer modificaciones, por ejemplo, el RENIEC tiene tiene aplicaciones que usan la biometría, ¿no? Habría que ver también cómo se captaría esa biometría, si serían sólo patrones numéricos o cómo resguardar esa información la empresa, pero obviamente hay un riesgo de que ante una brecha de seguridad esos datos queden expuestos. Bueno, la cuarta pregunta es ¿qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas? Bueno, primero, como te mencionaba la proporcionalidad, que estemos seguros que realmente necesitamos y es indispensable contar con el dato biométrico. Esa es la primera pregunta que hay que hacer. ¿Realmente necesitamos el dato biométrico o podemos resolver la situación con otro tipo de verificación? Segundo, mirar si estamos en alguna de las excepciones del artículo 14 de la ley para captar esos datos incluso sin el consentimiento del trabajador. Ya en Europa se ha dicho que el tema de fiscalización laboral no es una causal suficiente para la captación de esos datos sin el consentimiento del trabajador. Tercero, si se va a captar el dato biométrico tiene que cumplir con todas las características del consentimiento, sea libre, previo, expreso e informado. Entonces tengo que informarle claramente al trabajador para qué se van a utilizar esos datos, si se van a hacer transferencias internacionales, por cuánto tiempo se van a mantener almacenados, todo, todo. Cuarto, mantener niveles de seguridad altos respecto a esos datos, si se puede encriptarlos, tenerlos bajo un resguardo de altas medidas de seguridad. Y el segundo, eliminar esos datos una vez que ya no sean necesarios.

4. ¿Qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas?¿Cuál es su opinión sobre el uso de la inteligencia artificial en las cámaras de videovigilancia en el Perú y su impacto en la privacidad de los ciudadanos?

   Yo ahí sí considero que eso es un tema que debería ser prohibido u objeto de una regulación especial, porque el barrido biométrico con inteligencia artificial en tiempo real es algo que es cuestionado en distintos ámbitos, ¿no? En el Tribunal de Justicia de la Unión Europea, distintas autoridades de datos se han pronunciado al respecto, el mismo reglamento de inteligencia artificial de la Unión Europea lo acota a supuestos bien específicos, ¿no? Eso debería ser por un mandato judicial, por tiempos determinados, con un sustento suficiente. Porque tú sabes que el tema tiene muchos riesgos vinculados a sesgos discriminatorios, a falsos positivos, que pudieran terminar vulnerando derechos de las personas solo por encajar en algún tipo de perfil racial, hasta de nación étnico, qué sé yo, ¿no? Entonces eso sí yo creo merece que sea muy bien estudiado, regulado especialmente de ser el caso y que tenga un control, porque el ciudadano, ¿cómo va a tener una seguridad que esos datos estén siendo tratados correctamente? Esto incluso puede hasta atentar contra la libertad de expresión, porque al saber que por todos lados te están haciendo barridos biométricos, tú te puedes inhibir incluso hasta ejercer tu derecho de protesta, ¿no? Entonces ahí hay varios temas peligrosos que ameritan, sí yo creo, una visión particular y de ser el caso o una prohibición o una regulación especial, que sea garantista de derechos.

ENTREVISTA 3:

Fecha: 28 de febrero del 2025

Hora: 17:00 p.m

Lugar: Lima, Perú

Entrevistado: Marìa Camargo Román - Ingeniera especializada en Sistemas e Informática con mención en Dirección en TI, con formación en la Pontificia Universidad Nacional Mayor de San Marcos.

1. ¿Está familiarizado con la Ley N° 29733, ley que protege los datos personales? ¿Cree que debería existir una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos?

   Si estoy familiarizada con la Ley N° 29733. El concepto no es claro, debemos precisar "USO" y "ENTRENAMIENTO", para el USO el termino es muy difuso porque son simplemente datos como cualquier otro, ya depende de la aplicación que se requiera la IA proporcionara la información que necesita un usuario. Caso ENTRENAMIENTO, lo datos biométricos en específico, es decir un DNI, Huella Digital, Iris, Rostro, etc., es casi irrelevante para en entrenamiento, ya que son datos, por ejemplo, entrenar con DNI basta saber que tiene ocho dígitos, entonces la IA se entrena con un valor de 8 dígitos y aprende que un DNI debe tener 8 dígitos para un formulario en específico, igual manera pude suceder con un rostro, un Iris, etc. El enfoque es si alguien da acceso no autorizado a utilizar base de datos de las personas. Pero en ese caso no es un problema que pueda involucrar a la IA es quien entrega la información. Por lo tanto, no se debe legislar en específico para la IA.

2. ¿Existe asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos? ¿Considera que esta falta de transparencia limita la posibilidad de tomar decisiones informadas sobre su uso?

   Confirmo que es ilegal recopilar datos sin el conocimiento o consentimiento adecuado de los individuos. Desde el punto de vista quien obtiene estos datos en forma ilegal como la mencionada, es claro que existe un gran riesgo de tomar decisiones que involucra dinero, tiempo y otros recursos. Las personas afectadas pueden tomar acciones por violar sus derechos a la privacidad.

3. Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo considera que una violación de seguridad podría afectar la privacidad de los trabajadores en el ámbito laboral?

   En especifico los datos "BIOMETRICOS" se refiere a las características biológicas de las personas, como son, rostro, Iris, Huella Digital, La voz que actuales tecnologías tienen capacidad de capturar como datos y convertirlos en

valores de identificación, en general este tipo de datos se utilizan para el ACCESO SEGURO UNICO de las personas, entonces la violación de seguridad esta dirigida a los acceso que puede tener un individuo a diferentes procesos de identificación que puede utilizar, por ejemplo, ingreso al trabajo, acceso a información médica, operaciones bancarias, y otras actividades que utilicen biometría para permitir el acceso. Por lo tanto, desde el punto de vista de seguridad a suplantación de identidad constituye un riesgo serio a la seguridad.

4. ¿Qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas?¿Cuál es su opinión sobre el uso de la inteligencia artificial en las cámaras de videovigilancia en el Perú y su impacto en la privacidad de los ciudadanos?

   Como ya se mencionó, los datos biométricos son inherentes al cuerpo humano, y se llevan consigo a cualquier lugar donde nos desplacemos, entonces la captura de datos biométricos a lo que se refiere la pregunta solo debe ser indicada en procesos donde es necesaria 100% de seguridad de identificación, donde sea necesario confirmar la identidad en forma física, por lo tanto no debe ser necesario exigir datos biométricos en casos donde es suficiente otros medio de identificación, por ejemplo ingreso al trabajo, solo debería ser suficiente una tarjeta de identificación, o ingreso a un gimnasio o cualquier otra actividad de esparcimiento, no justifica la biometría ya que esto puede exponer la seguridad de las personas.

   Con referencia de la aplicación de IA en cámaras CCTV, es limitado la que puede ofrecer ya que la tecnología de reconocimiento facial es casi nula en la aplicación de identificación en la vía publica, la razón es que los resultados se basan en la probabilidad que una captura de imagen puede ser una persona y los rangos máximos son de 90-95% para los casos de reconocimiento facial en oficinas o lugares donde las personas están obligadas a identificarse y la cámara tiene una línea de vista. En la vía publica es inaplicable la identificación, los niveles de error son de 30 – 50% solo “SI” se tiene una base de datos de la imagen del individuo que debe ser actualizada y no tener ningún tipo de objeto (lentes, gorros, vichas, etc.) o características propia de la

persona (barba, color de la piel, tamaño del cabello, etc.) , como es público no existe alguna base de datos con fotos de las personas para se puedan utilizar, es común encontrar comentarios de que la RENIEC tiene las fotos , pero esos datos no tienen ninguna utilidad es inservible para la tecnología de reconocimiento facial, la IA no puede ser categórica en certificar quien es la persona de una imagen de cámara CCTV.

ENTREVISTA 4:

Fecha: 05 de marzo del 2025

Hora: 12:00 p.m

Lugar: Lima, Perú

Entrevistado: Josesaúl Casas Chusho - Abogado especialista en Derecho Laboral, con formación en la Universidad Nacional de Trujillo. Actualmente, ejerce funciones como secretario judicial en la Tercera Sala Laboral de la Corte Superior de Justicia de La Libertad.

1. ¿Está familiarizado con la Ley N° 29733, ley que protege los datos personales? ¿Cree que debería existir una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos?

Tengo conocimiento general de la norma mencionada; sin embargo, considero que es esencial promulgar una regulación específica sobre el uso de la inteligencia artificial en la gestión de datos biométricos. Estos datos, al ser considerados información sensible, requieren una protección reforzada para salvaguardar la privacidad y los derechos fundamentales de las personas. Además del componente ético que implica su tratamiento, una normativa clara ayudaría a prevenir posibles vulneraciones y a mitigar riesgos asociados a la ciberseguridad, garantizando así un equilibrio entre la innovación tecnológica y la protección de la dignidad humana

2. ¿Existe asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos? ¿Considera que esta falta de transparencia limita la posibilidad de tomar decisiones informadas sobre su uso?

Claro que existe una asimetría de información cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos. La falta de información y transparencia puede generar un uso indebido de estos datos, dejando a las personas en una posición de vulnerabilidad frente a posibles abusos o tratamientos desproporcionados de su información personal.

Esta brecha de conocimiento limita gravemente la capacidad de los individuos para tomar decisiones informadas sobre el uso de sus datos, impidiendo que puedan ejercer plenamente sus derechos. Por eso, considero esencial que existan mecanismos claros de información y consentimiento, así como normativas que garanticen la protección de la privacidad y promuevan la confianza en el uso de estas tecnologías.

3. Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo considera que una violación de seguridad podría afectar la privacidad de los trabajadores en el ámbito laboral?

Las violaciones de seguridad afectan directamente a los trabajadores, no solo en el ámbito laboral, sino también en su esfera privada. Dado que los datos biométricos son únicos, permanentes y prácticamente imposibles de modificar, su exposición podría derivar en graves consecuencias, como fraudes, suplantación de identidad o estafas. Además, la filtración o divulgación de esta información sensible podría generar un impacto emocional y psicológico en los trabajadores, al sentir que su privacidad ha sido vulnerada de forma irreversible.

Por esta razón, considero que es fundamental que las empresas adopten medidas de ciberseguridad robustas, con protocolos claros para prevenir y gestionar incidentes, garantizando así la protección de los derechos y la integridad de los trabajadores frente a posibles amenazas digitales

4. ¿Qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas?¿Cuál es su opinión sobre el uso de la inteligencia artificial en las cámaras de videovigilancia en el Perú y su impacto en la privacidad de los ciudadanos?

Considero que el uso de la inteligencia artificial puede ser muy beneficioso si se implementa de manera responsable y bajo parámetros claros. En el contexto

actual de creciente inseguridad ciudadana, creo que sería factible y efectivo utilizar la inteligencia artificial en cámaras de videovigilancia en espacios públicos para optimizar el rol de la seguridad ciudadana. Esto permitiría identificar a los delincuentes con mayor rapidez y facilitar su arresto, contribuyendo así a la protección de la población.

Sin embargo, soy consciente de que, aunque no podemos ignorar los beneficios de esta tecnología, es fundamental establecer límites precisos y regulaciones estrictas para evitar que el uso de datos biométricos vulnere los derechos fundamentales de las personas. La implementación de estas herramientas debe ser proporcional y siempre respetar el derecho a la privacidad y la protección de los datos personales, buscando un equilibrio adecuado entre la seguridad pública y las libertades individuales.

ENTREVISTA 5:

Fecha: 07 de marzo del 2025

Hora: 13:00 p.m

Lugar: Lima, Perú

Entrevistado: Lyanee Pineda Abuhadba - Abogada por la PUCP asociada en el Esfudio Bellido Abogados, donde lidera el área laboral del estudio.

1. ¿Está familiarizado con la Ley N° 29733, ley que protege los datos personales? ¿Cree que debería existir una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos?

Sí, estoy familiarizada con la Ley N° 29733, que protege los datos personales. Considero que es fundamental que exista una regulación específica para el uso de la inteligencia artificial en el uso de datos biométricos, ya que estos datos son especialmente sensibles y requieren una protección pendiencia de especial y sobre si en el ámbito laboral ya que muchas veces se comparte información con empresas que prestan servicios, o por darles beneficios a los propios trabajadores.

2. ¿Existe asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos? ¿Considera que esta falta de transparencia limita la posibilidad de tomar decisiones informadas sobre su uso?

Sí, existe una asimetría de información y poder cuando los datos biométricos son recopilados sin el conocimiento o consentimiento adecuado de los individuos. Esta falta de transparencia limita significativamente la posibilidad de tomar decisiones informadas sobre su uso, lo que puede generar riesgos para la privacidad y la seguridad de los trabajadores, pues las empresas pueden acceder a información confidencial que esta dentro de esfera personal. Habria que revisar las politicas internas de las empresas para revisar los límites del acceso a esta información

3. Dado que los datos biométricos son permanentes y difíciles de modificar, ¿cómo considera que una violación de seguridad podría afectar la privacidad de los trabajadores en el ámbito laboral?

Una violación de seguridad que afecte los datos biométricos podría tener consecuencias devastadoras para la privacidad de los trabajadores en el ámbito laboral, pues puede generar incluso una suerte de inseguridad en los procesos, por ejemplo para el registro de ingreso y salida, hasta generar acceso a informacion que solo le compete a cierto grupo de empresa. Ademas que tambien podría generar riesgos de identificación, discriminación, entre otros.

4. ¿Qué medidas considera necesarias para asegurar que el uso de datos biométricos no vulnere los derechos fundamentales de las personas?¿Cuál es su opinión sobre el uso de la inteligencia artificial en las cámaras de videovigilancia en el Perú y su impacto en la privacidad de los ciudadanos?

Para asegurar la protección de los datos biométricos, considero necesarias las siguientes medidas:

- Implementar políticas de privacidad y seguridad claras y transparentes, siempre recogiendo el consentimiento del trabajador

- Obtener el consentimiento informado y explícito de los trabajadores antes de recopilar y utilizar sus datos biométricos, por la sensibilidad que existe con los hackers o robo de información.

- Implementar medidas de seguridad adecuadas para proteger los datos biométricos contra violaciones y accesos no autorizados de los datos de los trabajadores

- Establecer procedimientos para notificar y responder a incidentes de seguridad que afecten los datos biométricos, y cuales serian sus consecuencias a nivel laboral.

- Realizar auditorías y evaluaciones periódicas para garantizar la cumplimiento con las regulaciones y políticas de privacidad y seguridad, para evitar la fuga de información