UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

EL TRATAMIENTO DE DATOS PERSONALES BIOMÉTRICOS DENTRO DE ENTORNOS LABORALES EN EL MARCO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES FRENTE AL PRINCIPIO DE LEGALIDAD.

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

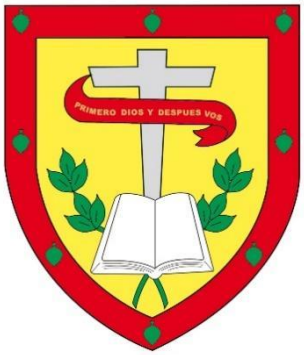
AUTOR: MATEO JOSUE CARCHIPULLA FAJARDO

DIRECTORA: ABG. MÓNICA CECIBEL GALLEGOS AVENDAÑO, MGS

CUENCA – ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

EL TRATAMIENTO DE DATOS PERSONALES BIOMÉTRICOS DENTRO DE ENTORNOS LABORALES EN EL MARCO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES FRENTE AL PRINCIPIO DE LEGALIDAD.

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

AUTOR: MATEO JOSUE CARCHIPULLA FAJARDO

DIRECTORA: ABG. MÓNICA CECIBEL GALLEGOS AVENDAÑO, MGS

CUENCA – ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLO

Universidad Católica de Cuenca	DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD	CÓDIGO: F – DB – 34 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Mateo Josue Carchipulla Fajardo portador de la cédula de ciudadanía **N° 0150051399.** Declaro ser el autor de la obra: **"El tratamiento de datos personales biométricos dentro de entornos laborales en el marco de la Ley Orgánica de Protección de Datos Personales frente al principio de legalidad.",** sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, 28 de noviembre del 2025

F.....

Mateo Josue Carchipulla Fajardo

C.I 0150051399

Universidad Católica de Cuenca

CERTIFICO

Yo, **Mónica Cecibel Gallegos Avendaño** certifico que el presente proyecto de titulación con el título "**El tratamiento de datos personales biométricos dentro de entornos laborales en el marco de la Ley Orgánica de Protección de Datos Personales frente al principio de legalidad**", fue desarrollado por **Mateo Josue Carchipulla Fajardo**, bajo mi supervisión.

F: .....

Abg. Mónica Cecibel Gallegos Avendaño, Mgs

Docente - Tutor

Dedicatoria

A Meel Ferias, por ser una fuente constante de apoyo, inspiración y paciencia en cada etapa de este camino. Gracias por creer en mí incluso en los días más difíciles y por recordarme siempre que los sueños sí se construyen con esfuerzo y corazón. Este logro también es tuyo.

Agradecimiento

A mi familia, por su amor incondicional y por enseñarme, con su ejemplo, el valor del trabajo, la disciplina y la perseverancia. Gracias por cada palabra de aliento, por cada sacrificio silencioso y por estar presentes en cada paso de este proceso. Sin ustedes, este logro no habría sido posible.

Resumen

La investigación analiza el tratamiento de los datos personales biométricos dentro de entornos laborales ecuatorianos, a la luz del principio de legalidad y de la Ley Orgánica de Protección de Datos Personales (2021). Este estudio examina la tensión entre la necesidad de control empresarial y la garantía de derechos fundamentales, destacando la relevancia de la autodeterminación informativa y la dignidad humana. Los datos biométricos, por su carácter único e inmutable, requieren una protección reforzada, pues su uso indebido puede vulnerar la privacidad y generar discriminación o control indebido sobre los trabajadores. La Constitución de 2008 reconoció por primera vez en el país el derecho a la protección de datos personales, mientras que la creación de la Superintendencia de Protección de Datos Personales en 2023 marcó un avance institucional aún incipiente. El trabajo compara la normativa ecuatoriana con estándares internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y las directrices de la OCDE, evidenciando la necesidad de fortalecer la supervisión, la proporcionalidad y el consentimiento libre en las relaciones laborales. Se concluye que la efectividad de este derecho depende de su aplicación real, la capacitación institucional y la consolidación de una cultura jurídica que priorice la protección de la privacidad en el ámbito laboral y tecnológico.

Palabras clave: *datos biométricos, legalidad, confidencialidad, consentimiento, tratamiento de datos.*

Abstract

The research analyzes the processing of biometric personal data within Ecuadorian work environments, in light of the principle of legality and the Organic Law on Personal Data Protection (2021). This research examines the conflict between the need for corporate control and the guarantee of fundamental rights, highlighting the importance of informational self-determination and human dignity. Biometric data, due to its unique and immutable nature, requires enhanced protection, as its misuse can violate privacy and lead to discrimination or undue control over workers. The 2008 Constitution recognized the right to personal data protection for the first time in the country, while the establishment of the Superintendency of Personal Data Protection in 2023 marked an institutional advance that is still in its beginnings. The research compares Ecuadorian regulations with international standards such as the European Union's General Data Protection Regulation (GDPR) and OECD guidelines, highlighting the need to strengthen oversight, proportionality, and free consent in labor relations. It concludes that the effectiveness of this right depends on its actual application, institutional training, and the consolidation of a legal culture that prioritizes privacy protection in the labor and technological spheres.

Keywords: *biometric data, legality, confidentiality, consent, data processing.*

Índice

Introducción

La atención que se ha prestado a los datos personales y, sobre todo, a los datos biométricos, ha permitido traer a la discusión contemporánea temas sobre la privacidad y derechos fundamentales en el tejido social del siglo XXI. Además del valor puramente tecnológico que conlleva, este tratamiento configura el respeto y la protección de la dignidad, autonomía y privacidad de las personas, en especial en cuestiones del trabajo. Para el caso de Ecuador, la Constitución de 2008 fue la primera en el mundo en reconocer el derecho a la protección de datos personales, y sentó las bases de un ordenamiento que fue deficitario, hasta la publicación en 2021 de la Ley Orgánica de Protección de Datos Personales. Esta ley formalmente empezó a regular el tratamiento de datos en el país, sin embargo, su aplicación -sobre todo en datos biométricos en el trabajo- sigue siendo problemática.

Los biométricos tienen características como los patrones de huellas dactilares, reconocimiento facial y patrones de voz y, lo que los hace aún más interesantes, pueden identificar de forma permanente e irremediablemente a una persona. Esta singularidad otorga a los biométricos una sensibilidad que, si no se administran correctamente, les pueden generar grandes riesgos a los derechos de los titulares. En este sentido, el principio de legalidad se presenta como un faro.

A nivel mundial, el derecho a la protección de datos personales se considera un derecho fundamental, posición que también ha querido defender Ecuador. La Ley Orgánica de Protección de Datos Personales, que en el ámbito de la protección de datos personales se ha equiparado a la legislación de la Unión Europea (Reglamento General de Protección de Datos), establece ciertas condiciones para la protección de datos personales, sin embargo, la falta de supervisión práctica, así como el escaso nivel de capacitación en las instituciones responsables la hacen poco operativa. La creación en 2023 de la Superintendencia de

Protección de Datos Personales ha sido un avance para el reconocimiento y ejercicio de este derecho, sin embargo, todavía se requiere un mayor esfuerzo en la implementación de acciones que hagan efectivo este derecho.

Este analisis aborda la cuestión del uso de datos biométricos en el contexto laboral de la Ley Orgánica de Protección de Datos Personales de Ecuador, y sobre los aspectos legales, éticos y prácticos de su aplicación, incorporando una visión crítica. También se realiza una aproximación comparativa de la normativa ecuatoriana en la región y en el contexto de estándares internacionales, poniendo mayor énfasis en la falta de tutela de derechos fundamentales en escenarios de globalización y en la digitalización de datos interconectados. Se busca, a través de este trabajo, comprender y dimensionar el desbalance en la normatividad ecuatoriana y plantear los lineamientos fundamentales que permitan su correcta y efectiva implementación, en relación a la tutela de datos biométricos en el trabajo.

El estudio subraya la importancia de un enfoque integral en la protección de los datos personales, que no solo se base en la existencia formal de normativas, sino que también garantice su aplicación efectiva y proactiva, tanto en el sector público como en el privado, promoviendo una cultura de respeto a la privacidad y seguridad de los datos de los ciudadanos.

Capitulo I

Marco normativo de la Ley Orgánica de Protección de Datos Personales y su relación con el principio de legalidad en el tratamiento de datos personales biométricos.

1.1. La constitucionalización de los derechos de protección de datos personales

El origen de este derecho remonta su vuelo a 1970, cuando el

Tribunal Constitucional Alemán resolvió un caso aparentemente técnico

un censo poblacional pero que acabaría marcando un antes y un después en la historia del derecho. Aquel fallo sentó el precedente del derecho a la autodeterminación informativa. Como señala Pablo Contreras (2020) "*la autodeterminación informativa garantizaría la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales*". Con esta decisión, se abrió una puerta y se encendió una luz: la protección de datos debía entenderse como una extensión natural de la libertad individual. Años más tarde, en 1981, ese mismo espíritu se cristalizó en el Convenio 108 del Consejo de Europa, el primer tratado internacional que, como un faro, marcó el rumbo de la protección de datos como derecho humano fundamental.

América Latina no tardó en hacer eco de esa voz. En 1996, Argentina se convirtió en pionera al incluir en su Constitución el hábeas data, un recurso que le dio voz a los silencios, rostro a los olvidos y poder a los ciudadanos para acceder, corregir o eliminar su información personal. María Mercedes Serra (2001) destaca que el desarrollo jurisprudencial en América Latina ha consolidado el hábeas data como mecanismo eficaz frente a abusos estatales y privados. Esta figura jurídica inspiró movimientos constitucionales en varios países de la región, incluido Ecuador. En 2008, con la promulgación de una nueva Constitución, se sembró en nuestro texto constitucional la semilla de la protección de datos personales.

La Constitución de la República del Ecuador de 2008 no pasó de largo ni fue tímida: en su artículo 66, numeral 19, se reconoce el derecho a acceder, rectificar, eliminar y oponerse a la difusión de sus datos, sin importar si estos estaban en un papel, en una base digital o en la nube. Además, estableció que dicho tratamiento solo podía hacerse con un consentimiento previo, libre e informado. Esta disposición, como lo sostiene la Corte Constitucional del Ecuador (2020) establece que: "*toda información que haga referencia de forma directa o indirecta a cualquier aspecto relativo a una persona o sus bienes, en sus distintas esferas o dimensiones; susceptible de ser exigida a través de la garantía de hábeas*

data". Ecuador se unió al entorno global que defiende la autonomía del individuo frente al uso indiscriminado de sus datos.

La protección de los datos personales ha sido uno de los estandartes más firmes en la evolución jurídica de los derechos fundamentales del siglo XXI. Este es un derecho que va más allá de una simple formalidad legal; es una respuesta a la creciente e inmediata necesidad de proteger la dignidad, autonomía y privacidad de un individuo en una sociedad cada vez más digital, interconectada y orientada a la vigilancia. En Ecuador, la Constitución de 2008 sentó las bases legales para este derecho, que ha continuado avanzando reformas constitucionales gracias a los movimientos sociales cambiantes y a los marcos legales a niveles internacional y regional.

El reconocimiento de este derecho por la Constitución fue una formalidad que requería un marco legal para operativizarlo. Después de numerosos retrasos, 2021 finalmente vio la publicación e implementación de la Ley Orgánica de Protección de Datos Personales. Esta ley es mucho más que un conjunto de artículos: es un escudo normativo, un manual ético y una guía técnica para garantizar que el derecho a la protección de datos no quede en el papel. Dentro de sus disposiciones, se reconoce el carácter sensible de los datos biométricos, esa huella digital única que nos delata, ese rostro que las cámaras conocen, esa voz que los algoritmos graban, tal como lo establece el artículo 4 de la Ley Orgánica de Protección de Datos Personales, "*los datos biométricos personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona*" (Asamblea Nacional, 2021).

Un elemento fundamental que refuerza la constitucionalización del derecho a la protección de datos personales en Ecuador es su autonomía frente al derecho a la intimidad. Mientras el derecho a la intimidad se refiere a aspectos profundamente personales como las convicciones ideológicas, religiosas o la orientación sexual, el derecho a la protección

de datos personales abarca un espectro mucho más amplio, incluyendo toda información que identifique o pueda identificar a una persona, aun cuando no pertenezca a su esfera íntima (Reyes, 2016).

Asimismo, el concepto de autodeterminación informativa emerge como el eje central del contenido de este derecho. El individuo no solo tiene derecho a conocer qué datos existen sobre él, sino que también puede decidir qué información comparte, con quién y para qué propósito, consolidando así un poder de disposición sobre su propia identidad digital. Como señala Martínez (2004, citado en Reyes, 2016, p. 5), esta construcción traslada el fundamento del derecho desde una visión patrimonialista hacia una basada en la dignidad humana y la inviolabilidad de la personalidad.

Un aporte adicional de gran valor es la jurisprudencia internacional, especialmente de España y Alemania, que ha sido incorporada en la evolución del derecho en Ecuador. En la sentencia STC 292/2000 del Tribunal Constitucional Español se afirma que la protección de datos personales no se restringe a la intimidad, sino que cubre cualquier dato que, al ser tratado por terceros, pueda afectar derechos, sean o no fundamentales. En palabras de la propia Corte: "*los derechos de acceso, rectificación y cancelación... integran el derecho fundamental de todos a controlar la recogida y el uso de aquellos datos personales que pueden poseer tanto el Estado como los particulares*" (Tribunal Constitucional Español, 2000).En el caso ecuatoriano, un aspecto normativo importante fue la entrada en vigor de la Ley del Sistema Nacional de Registro de Datos Públicos en 2010, que, aunque no regula de forma íntegra el derecho constitucional, reconoce su existencia y establece principios rectores para el tratamiento de datos en registros públicos (Reyes, 2016). No obstante, este marco legal era insuficiente hasta la aprobación de la Ley Orgánica de Protección de Datos Personales en 2021.

El avance legal vino acompañado de una creación institucional. En 2023, nació la Superintendencia de Protección de Datos Personales, una

entidad que no solo supervisa y sanciona, sino que también vigila, orienta y protege. Esta autoridad representa el brazo operativo del derecho, el puente entre el principio y la práctica, entre la norma y la realidad. Su existencia concreta y la aspiración de que la protección de datos sea un derecho vivo, dinámico y efectivo, especialmente frente a los empleadores y empresas que recolectan información biométrica de sus trabajadores.

La constitucionalización del derecho a la protección de datos personales en Ecuador no fue un accidente ni una tendencia pasajera, sino el resultado de un proceso jurídico progresivo, cuidadosamente influenciado por experiencias internacionales y necesidades locales. La Constitución de 2008 le dio voz al derecho, la ley de 2021 le dio forma, y la autoridad de control de 2023 le dio fuerza. En un entorno donde los datos y en especial los biométricos se han convertido en la moneda de cambio del control y la eficiencia, la protección de esa información es más que necesaria: es una exigencia moral y jurídica. Porque proteger los datos personales es, en última instancia, proteger lo que somos.

1.2. Autoridad de la ley de protección de datos personales

En el marco del Estado constitucional de derechos y justicia, la autoridad de una norma jurídica no se limita a su existencia formal, sino que depende de su legitimidad constitucional, su capacidad para regular conductas y su eficacia para tutelar derechos. La Ley Orgánica de Protección de Datos Personales, aprobada en Ecuador en 2021, posee una autoridad derivada de su jerarquía normativa, su función como ley habilitante del derecho constitucional a la protección de datos personales y su integración dentro del sistema jurídico ecuatoriano.

Desde una perspectiva teórica, la autoridad normativa de una ley se refiere a su fuerza vinculante dentro del ordenamiento jurídico y a la legitimidad de su mandato sobre los destinatarios. Según Manuel Atienza (2006), una norma tiene autoridad no solo por su rango legal, sino también por el "*reconocimiento racional y voluntario de su contenido por parte de los ciudadanos y operadores jurídicos*".

El fundamento de esta autoridad, como ley orgánica, se encuentra en el artículo 133 de la Constitución, que establece que estas normas regulan el ejercicio de los derechos y las garantías constitucionales. Esto significa que la Ley Orgánica de Protección Datos Personales es una norma de desarrollo constitucional y, en consecuencia, de aplicación preferente a la de rango inferior. Esto último se encuentra por así recogerlo Carpetizo (1999), "*Las leyes orgánicas tienen la función de desarrollar y delimitar los derechos fundamentales, especificando su contenido y los límites dentro del marco constitucional*".

Esta ley, por su parte, asume la función de ley habilitante en el sentido de que hace posible el ejercicio de un derecho que la Constitución reconoce, pero que, sin el desarrollo legislativo, su ejercicio es efectivo, inoperativo. A este respecto, resulta esencial la afirmación de Rubio Llorente (2006) en el sentido de que los derechos fundamentales requieren de un desarrollo jurídico que precise su contenido y límites a los efectos de que no se queden en meras declaraciones sin eficacia práctica.

La Ley Orgánica de Protección Datos Personales también muestra su autoridad con su eficacia normativa, es decir, su capacidad de impactar el tratamiento de datos en la práctica, jurídica, institucional y en la sociedad en general. La ley ofrece un conjunto integral de principios, obligaciones y sanciones que permiten ajustes que pueden ser aplicados de forma real y comprobable. Dentro de estos principios se consideran la licitud, finalidad, proporcionalidad, confidencialidad y responsabilidad proactiva. Su eficacia se apoya también en la consagración y reconocimiento de los derechos ARCOPOL (Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición), que permite un efectivo control y jurisdicción por parte de los ciudadanos sobre sus datos (Carbonell, 2021).

La autoridad de esta ley, también, por su función simbólica y pedagógica. Como lo menciona Carbonell (2021), una ley orientada a

derechos fundamentales en el ámbito digital, no solo impone obligaciones, también educa y genera cultura jurídica. En este sentido, la Ley Orgánica de Protección Datos Personales ayuda a nutrir una ética pública en el respeto a la información personal, más aún en el ámbito laboral, donde el uso de datos biométricos es común y cada vez más invasivo.

La Ley Orgánica de Protección de Datos Personales tiene como fundamento su respeto a la Constitución, su rango y jerarquía dentro del ordenamiento, la habilitación que la acción refiere, la eficacia de la norma en la práctica y la efectividad del argumento como resguardo de derechos fundamentales. La norma cuenta y tiene un carácter imperativo, decorativo ni simbólico, pues otorga y protege la dignidad, el derecho al consentimiento y el control del flujo de la información en el contexto de una sociedad digital.

1.3. Principios rectores de la Ley Orgánica de Protección de Datos Personales (LOPDP)

En el marco del Estado constitucional de derechos, los principios jurídicos van más allá de ser simples guías orientativas; son la base sobre la cual se construye e interpreta todo el sistema legal. En lo que se refiere a la Ley Orgánica de Protección de Datos Personales, estos son principios que son la base para que el respeto sobre el manejo de los datos personales se haga de forma digna, de forma sobre la autonomía individual y sobre los límites constitucionales. Para Carbonell (2021), los principios en la protección de datos son base para la normatividad en el derecho y logra un equilibrio entre el avance y la innovación de la tecnología y la protección de los derechos fundamentales.

En la Ley Orgánica de Protección de Datos Personales, en específico en su artículo 10, se contempla los principios que guiarán el trato de datos personales en el país, sin perjuicio de otros principios que contenga la Constitución, ya sean de carácter internacional o de rango superior.

Esos principios, en razón de la naturaleza del ordenamiento jurídico, son de cumplimiento obligatorio y, en consecuencia, garantizan la legalidad, legitimidad y proporcionalidad tanto en el ámbito público como en el privado del uso de la información personal. Por lo tanto, debe entenderse como el mínimo garantizado el respeto de los derechos fundamentales y la constitución vigente en el ejercicio de actividades sobre datos personales.

El principio de juridicidad requiere que todo tratamiento de datos personales se lleve a cabo de acuerdo a lo que establece la Constitución, los tratados internacionales ratificados, la ley, su reglamento y la normativa y jurisprudencia pertinentes.

La juridicidad implica que ninguna actividad sobre datos personales puede realizarse al margen de una base legal expresa y legítima, y que los responsables y encargados de tratamiento están sujetos a los límites y condiciones que establece el marco jurídico. Este principio asegura el sometimiento pleno de las actuaciones relacionadas con datos personales al principio de legalidad, base del sistema constitucional ecuatoriano.

> Como sostiene Lorenzo Cotino Hueso, “el principio de legalidad o juridicidad supone que todo tratamiento de datos personales ha de fundarse en una norma jurídica clara, precisa y accesible, constituyendo una manifestación del sometimiento de la Administración y de los particulares al Derecho, en garantía del derecho fundamental a la protección de datos” (2019).

El tratamiento de datos debe realizarse con lealtad hacia el titular. Esto exige que la persona titular de los datos tenga conocimiento claro de que su información está siendo tratada, y de las formas en que ello ocurre. La ley prohíbe que los datos personales sean tratados mediante medios ocultos o con fines desleales, es decir, que el tratamiento no se comunique adecuadamente o se oriente a propósitos encubiertos, ilícitos o incompatibles con los derechos del titular.

A este principio se suma el de transparencia, el cual impone el deber de comunicar de forma accesible y comprensible toda la información relativa al tratamiento de datos personales. Las entidades responsables deben informar, en un lenguaje claro y sencillo, quién es el responsable, qué datos se recogen, con qué finalidad, por cuánto tiempo se conservarán y qué derechos tiene el titular respecto a su información. La profesora María Guerrero explica que "*mediante el cumplimiento de varias exigencias se pretende que la persona que consiente la recogida de sus datos tenga conocimiento del alcance exacto de sus actos*" (s.f.). Desde una perspectiva jurídica, este principio cumple una función garantista en el ejercicio del derecho a la autodeterminación informativa. En efecto, si el titular desconoce quién trata sus datos, para qué fines y bajo qué condiciones, se ve imposibilitado de ejercer sus derechos de forma efectiva. La cita de la profesora María Guerrero refuerza esta idea al subrayar que el consentimiento debe ser informado, es decir, debe basarse en un conocimiento real y suficiente de las consecuencias jurídicas y prácticas de entregar los datos.

El principio de finalidad establece que los datos personales deben tratarse únicamente para propósitos determinados, explícitos, legítimos y previamente comunicados al titular. María Serrano afirma que los datos personales recogidos deben estar vinculados con la finalidad que pretende alcanzar el fichero; si se altera dicha finalidad, los datos se convierten en inadecuados para su tratamiento. Pablo García Mexía señala que *"la determinación de la finalidad del tratamiento constituye el primer requisito para garantizar que el uso de los datos no se desvíe hacia objetivos distintos o incompatibles con los informados al titular, constituyendo así una salvaguarda básica frente a abusos*" (García Mexía, 2013). La ley también establece la obligación de tratar únicamente datos pertinentes y mínimos, adecuados a la finalidad para la que fueron recabados.

El principio de pertinencia y minimización implica que la recopilación de datos debe limitarse a aquellos estrictamente necesarios

para alcanzar el objetivo definido. Esto evita la recopilación de datos irrelevantes o excesivos y garantiza que el tratamiento de los datos se base en una finalidad inmediata y necesaria. Asimismo, el tratamiento de los datos debe ajustarse al principio de proporcionalidad, lo que significa que el uso de los datos debe ser pertinente, necesario, oportuno y no excesivo, en todos los casos relacionados con la finalidad legítima para la que fueron recopilados. Este principio es esencial en el caso de información sensible, especialmente datos biométricos. La proporcionalidad, que modera la discrecionalidad de los responsables del tratamiento, actúa como un escudo ético y legal. Gonzalo Álvarez García (2017) afirma: "*La proporcionalidad es una norma jurídica fundamental que exige el equilibrio de intereses potencialmente contrapuestos. Garantiza que las limitaciones impuestas a los derechos del interesado sean razonables y adecuadas, en correlación con la finalidad legítima que se pretende alcanzar"*. Esto tiene el efecto de prevenir abusos en el tratamiento de datos personales, particularmente cuando se trata de datos sensibles.

El principio de la confidencialidad establece que los datos tratados deben permanecer en secreto y que no pueden ser revelados, ni transferidos a otras multas, sin una razón que sea legal y pertinente. La persona a carga del tratamiento de datos debe tomar todas las medidas de orden técnico y organizativo necesarias para proteger la información confidencial, evitando que sea objeto de acceso no autorizado. Como señala Antonio Troncoso Reigada (2012), "*el principio de confidencialidad es un deber jurídico que recae sobre todos los actores… en el tratamiento de datos… de manera que los datos no salgan de los usos legales y de los fines que la ley establece*". Este principio se sostiene no solo en el derecho a la privacidad que la Constitución ampara, sino también en los derechos que los tratados internacionales reconocen. La protección de datos de forma física es solo una parte de los compromisos organizacionales. Se debe crear una cultura organizacional que promueva y respete la privacidad, incluso en los trámites administrativos rutinarios.

Los principios de calidad y exactitud de los datos son fundamentales en lo que respecta a la información personal. Los datos deben ser veraces, completos y, dentro de lo razonable, exactos y actualizados. María Guerrero afirma que la necesidad de que los datos reflejen la verdad determinará el valor del procesamiento automatizado. Cecilia Danesi (2020) también respalda esta idea al señalar que «la necesidad de veracidad y la actualización continua buscan eliminar las decisiones automatizadas y algorítmicas erróneas que pueden afectar negativamente los derechos del titular de los datos». Más allá de los matices técnicos, la calidad de la información y la precisión de las decisiones ponen de manifiesto la responsabilidad ética de garantizar el derecho a no verse perjudicado por datos erróneos. La ley subraya la necesidad de datos precisos, ya que el principio de exactitud exige que el procesamiento de datos sea legítimo y que los datos subyacentes sean exactos.

En cuanto a la retención de datos, el principio establecido fija que estos se conservarán únicamente durante el tiempo necesario para cumplir con la finalidad que justificó su recopilación. Una vez alcanzada dicha finalidad, el responsable del tratamiento deberá desactivar, eliminar o realizar revisiones periódicas del conjunto de datos. No obstante, con la debida justificación, en determinados casos se podrá permitir la retención de datos durante un período adicional con fines históricos, estadísticos o científicos. A este respecto, Juan Antonio García Amado (2018) sostiene que "*el principio de limitación temporal responde a una concepción altamente protectora de los derechos fundamentales, según la cual los datos solo pueden conservarse mientras la finalidad que justifica su retención siga siendo legítima y proporcional*".

La seguridad implica proteger los datos personales mediante acciones técnicas, organizativas y administrativas. En Ecuador, la Ley Orgánica de Protección de Datos Personales y, similarmente, la Ley Orgánica 3/2018 de Protección de Datos medidas de España señalan la necesidad de adoptar medidas efectivas para la protección de datos

personales de la modificación, pérdida y acceso no autorizado. En consecuencia, la responsabilidad proactiva o "rendición de cuentas" se convierte en principio básico.

> La rendición de cuentas va más allá de la implementación de medidas preventivas y correctivas, a aumentar la obligación de demostrar ante las autoridades competentes y los titulares de los datos que el tratamiento de datos se ajusta a los requisitos legales ya los principios de protección (Víctor Domingo, 2017).

Con relación al principio final, la interpretación a favor del titular del derecho se traduce, en caso de contradicciones, en la obligación de interpretar las normas de protección de datos en la forma más benigna posible para el titular. Este principio se articula, en el ámbito de la Constitución y el derecho internacional de los derechos humanos, con el principio pro persona y la garantía de los derechos fundamentales, en su sentido más amplio, la protección de los derechos fundamentales y la efectiva frente a las posibles ambigüedades o lagunas legales. Esta ambigüedad debe ser dirimida a favor del titular, como sostiene Santiago García (2015) "*la interpretación a favor del titular del derecho es un mecanismo que opera en el sentido de la protección de los derechos fundamentales, frente a ambigüedades o lagunas jurídicas, así garantizando la protección efectiva*".

Finalmente, el principio de independencia de control establece que la autoridad de protección de datos debe actuar con completa autonomía, imparcialidad y eficacia en el desempeño de sus funciones. Este principio refuerza a la autoridad de protección de datos al asegurar que sea un defensor activo del derecho, y no meramente una autoridad declarativa. Según María Rodríguez, "*la autonomía e independencia de la autoridad de control son indispensables para garantizar la confianza ciudadana y la efectividad de la protección de los datos personales*" (2018).

1.4. Alcance del principio de legalidad en el tratamiento de datos personales

De acuerdo con la Constitución de la República del Ecuador, en su artículo 226, las instituciones del Estado, sus funcionarios y cualquier entidad que ejerza potestad pública solo pueden actuar en virtud de la competencia que les confiere la ley. Esta previsión se extiende al tratamiento de datos personales, al punto de que la Ley Orgánica de Protección de Datos Personales, en su artículo 10, literal a), consagra como primer principio rector la juridicidad, estableciendo que los datos personales deben tratarse con estricto apego a la Constitución, los instrumentos internacionales de derechos humanos, la ley, su reglamento y demás normativa aplicable.

El principio de legalidad, en este contexto, implica que ninguna base de datos, procedimiento de recolección, análisis, almacenamiento o transferencia de datos puede realizarse sin contar con una norma habilitante legítima, esto es, una disposición que autorice explícitamente el tratamiento, defina su finalidad, delimite su alcance y establezca garantías adecuadas. Como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respeta al tratamiento de datos personales ya la libre circulación de dichos datos (Reglamento General de Protección de Datos - RGPD) "*El tratamiento será lícito solo si y en la medida en que se aplique al menos una de las siguientes condiciones: a) el interesado ha dado su consentimiento para el tratamiento de sus datos personales […]*" (Parlamento Europeo y del Consejo, 2019). El principio de legalidad proporciona un equilibrio contra la discrecionalidad y el abuso respecto a datos personales, asegurando que todo tratamiento se lleve a cabo dentro de un marco legal que se encuentre delimitado.

A nivel internacional, el Reglamento General de Protección de Datos de la Unión Europea se construye sobre el principio de legalidad como uno de sus pilares. En el artículo 6 se establece que, para que el tratamiento de datos se considere lícito, se deberá cumplir alguna de las

condiciones que se enumeran, tales como el consentimiento expreso de la persona interesada, el cumplimiento de alguna obligación legal, la ejecución de un contrato o la protección de intereses vitales. Este modelo normativo se ha reproducido en la Ley Orgánica de Protección de Datos Personales, donde en los artículos 7 a 9 establece las 'hipótesis de tratamiento legítimo' que describen las condiciones en que se puede realizar el tratamiento de datos sin quebrantar el principio de legalidad.

El alcance del principio de legalidad incluye, además, la sola existencia de una norma formal que habilite el tratamiento de datos. Es necesario que esa norma formal cumpla con ciertos estándares de calidad. La norma debe ser precisa, debe ser accesible, debe ser proporcional y debe ser predecible. De esta manera, una norma vaga y, por tanto, general, no podría ser considerada una base jurídica válida para el tratamiento de datos. Como lo ha sostenido Luigi Ferrajoli (2001), el ámbito de la legalidad en torno a los derechos fundamentales trasciende a la mera existencia formal de la norma, debiendo esta ser racional, coherente y capaz de proteger al ciudadano del poder.

El principio de legalidad, por lo tanto, se erige como uno de los pilares más importantes del orden constitucional moderno y tiene efectos en relación con los datos personales en cuestión. Dentro de un estado de derecho democrático, dicho principio se basa en que cualquier acto que influya en la situación de los individuos particularmente en los derechos fundamentales debe estar especificado y justificado en una legislación razonable, clara y preexistente. Mientras que la legislación sobre protección de datos esté en el caso del principio de legalidad, la información solo se procesa cuando la ley lo permite y de una manera predeterminada.

En el ámbito del manejo de datos personales, esto implica que no se puede simplemente citar una disposición reglamentaria o una cláusula contractual que autorice la disposición de manejo de datos. Debe quedar establecido explícitamente en la norma habilitante qué datos se

manejarán, los fines del tratamiento de datos, la identidad del responsable del tratamiento, el período durante el cual se almacenarán los datos, y los derechos del interesado. De lo contrario, se constituye la violación del principio de legalidad, incluso en presencia de entidades públicas, procesamiento automatizado o intervenciones públicas.

Así, la legalidad del tratamiento de datos, en el sentido legal, depende adicionalmente de la legalidad constitucional que garantiza la no infracción de derechos fundamentales en su funcionamiento. Así, por ejemplo, la Corte Interamericana de Derechos Humanos manifiesta que el consentimiento como base legal debe reunir condiciones sustantivas: debe ser libre, informado, específico, inequívoco y revocable. Cualquier tratamiento basado en un consentimiento viciado por omisión de información, presión contractual, o ausencia de alternativas es ilegal, aun cuando haya una manifestación formal de voluntad. En consecuencia, el principio de legalidad no puede ser entendido como un formalismo, sino como una garantía sustantiva del derecho a la autodeterminación informativa (Super Intendencia de Protección de Datos Personales, 2025).

La jurisprudencia ecuatoriana ha ratificado este entendimiento. En su Sentencia No. 182-15-SEP-CC, la Corte Constitucional sostuvo que la protección de datos personales exige el cumplimiento estricto del principio de legalidad y el tratamiento debe estar fundado en una norma legal clara que establezca los límites del uso, la finalidad y las garantías, siendo que es clara cuando dice que: “*La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.*”(Corte Cortistucional, 2015). Esto cobra especial importancia en entornos laborales, donde el uso de datos biométricos, sistemas de videovigilancia o plataformas digitales implica un tratamiento intensivo de datos personales y debe ser regulado de forma estricta.

1.5. Naturaleza jurídica de los datos biométricos en la Ley Orgánica de Protección de Datos Personales

La evolución de las tecnologías de identificación ha generado nuevas formas de tratamiento de datos personales que requieren una respuesta normativa precisa. Entre estas, los datos biométricos ocupan un lugar central, debido a su capacidad para identificar de forma directa, permanente e inequívoca a una persona. En este contexto, la Ley Orgánica de Protección de Datos Personales del Ecuador reconoce explícitamente a los datos biométricos como una categoría especial de datos personales, asignándoles un régimen jurídico reforzado dada su sensibilidad y su alta capacidad de riesgo para los derechos de los titulares.

De acuerdo con el artículo 4 de la Ley Orgánica de Protección de Datos Personales, se entiende por dato biométrico aquel "*relativo a las características físicas, fisiológicas o conductuales de una persona natural, que permiten o confirman la identificación única de dicha persona, como por ejemplo imágenes faciales, datos dactiloscópicos, voz, patrones de marcha, entre otros*" (Asamblea Nacional, 2021). Esta definición es consistente con la dada por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, cuyo artículo 4.14 define los datos biométricos como "*los datos personales obtenidos mediante un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permiten o confirman la identificación única de esa persona*" (Parlamento Europeo y Consejo de la Unión Europea, 2016) , por ende además de su valor identificatorio, los datos biométricos tienen una naturaleza altamente sensible debido a que, a diferencia de otros datos personales, no pueden ser modificados o sustituidos en caso de vulneración**.**

Desde la perspectiva jurídica, los datos biométricos no solo constituyen datos personales, sino datos de naturaleza altamente sensible, lo que les confiere una protección superior dentro del régimen legal. Además, la ley los clasifica como datos sensibles, junto con otros

datos cuya divulgación puede atentar contra los derechos fundamentales o libertades del titular. No se trata simplemente de una justificación, sino de una auténtica base de legitimidad. El reconocimiento normativo impone deberes reforzados para aquellos que tratan los datos personales, destacándose entre ellos la implementación de mecanismos de seguridad más rigurosos, la exigencia de un consentimiento informado, expreso y específico, y la obligación de basar el tratamiento en una de las causales de licitud que la normativa aplicable contempla de manera explícita.

Mientras que otros tipos de datos personales, como el nombre, la dirección o el número telefónico, pueden modificarse, los datos biométricos son una parte esencial de la identidad física de una persona y no pueden alterarse sin comprometer su integridad. Por esta razón, su tratamiento conlleva un riesgo considerablemente mayor para los derechos fundamentales, tales como la privacidad, la no discriminación, la integridad y la autodeterminación informativa.

> Sánchez-Castañeda y Márquez (2019), los datos biométricos, al ser inmutables y únicos, permiten crear sistemas de control permanente sobre los individuos, generando riesgos importantes para los derechos fundamentales como la privacidad, la libertad de movimiento y la libertad personal, especialmente cuando se integran en sistemas automatizados de vigilancia masiva.

El reconocimiento de la alta sensibilidad de los datos biométricos ha impulsado que diversas legislaciones y la doctrina exijan criterios estrictos para su tratamiento, buscando equilibrar la innovación tecnológica con la protección efectiva de los derechos humanos fundamentales. El Tribunal Europeo de Derechos Humanos ha advertido que el uso de tecnologías de control automatizado puede derivar en prácticas de perfilamiento discriminatorio y en un rastreo de personas sin su conocimiento. Asimismo, ha establecido que la videovigilancia debe ser pertinente, adecuada y no excesiva, debiendo garantizarse siempre el derecho a la información, así como el acceso y la seguridad de los datos

tratados (TEDH, Peck vs. Reino Unido, 2003; López Ribalda y otros vs. España, 2019).Este razonamiento se ve reflejado en normas como la Ley Orgánica de Protección de Datos Personales ecuatoriana, que trata los datos biométricos como sensibles, sujetos a bases legales reforzadas y protección granítica.

En el ámbito laboral, el tratamiento de datos biométricos es especialmente sensible, la recopilación de huellas dactilares, reconocimiento facial o análisis de voz como mecanismos de control de asistencia, acceso o productividad, plantea dudas sobre la proporcionalidad, la finalidad legítima y el consentimiento libre del trabajador. Tal como advierte "*El consentimiento dado en relaciones de subordinación como la contratación laboral no puede considerarse pleno, por lo que el uso de datos sensibles requiere bases jurídicas adicionales y justificación objetiva*" (García & López, 2018). En consecuencia, la Ley Orgánica de Protección de Datos Personales exige que los empleadores justifiquen claramente la necesidad de recolectar datos biométricos, evaluando su compatibilidad con los principios de legalidad, finalidad, proporcionalidad y minimización.

La Constitución de Ecuador reconoce el derecho a la privacidad y la protección de datos personales como parte de los derechos fundamentales de la Constitución. Este documento fundamental garantiza que el tratamiento de datos personales sea legítimo solo con el consentimiento expreso del titular, o cuando exista un mandato legal expreso. Esta es tanto una garantía sustantiva como un escudo contra cualquier tratamiento de datos personales que sea injustificablemente legal. Protege la dignidad humana, la autonomía y la privacidad de las personas contra el acceso no autorizado de entidades tanto públicas como privadas. Desde este ángulo, la ley de protección de datos personales permite a las personas reclamar protección legal contra cualquier infracción injusta de los derechos fundamentales.

La Ley Orgánica de Protección de Datos Personales, a pesar de su carácter confidencial, establece una clasificación básica de los datos personales en dos categorías: datos personales generales y datos personales especiales. Los datos personales generales son aquellos que permiten identificar a una persona y que comprenden su nombre, apellido, dirección y estado civil. El tratamiento de estos datos es importante, pero no implica una gran intromisión en la vida privada de la persona. En cambio, el tratamiento de los datos personales especiales puede constituir, en gran medida, una violación del derecho a la seguridad de las personas. Dentro de estos, se encuentran, entre otros, los datos considerados sensibles, datos de salud, información y datos de personas discapacitadas, dependientes, menores, datos no acotados, en algunos casos, información de personas fallecidas, datos de personas con enfermedad mental, y en algunos casos, datos de personas con enfermedad mental (Asamblea Nacional, 2021).

Los datos personales sensibles son aquellos que afectan profundamente la intimidad, la integridad física o moral, y las creencias de una persona. Según la legislación, los datos biométricos también son parte de esta subcategoría, por lo que estos datos también y requieren especialmente de un régimen de protección. Esto implica que su tratamiento no se deba hacer de forma habitual y que no existe una justificación legal. La diferencia en la clasificación de los datos no es una cuestión puramente formal, sino la forma de establecer un orden. En este, el tratamiento de datos sensibles se reconoce como prohibido y el artículo 26 referente al tratamiento de datos personales (Asamblea Nacional, 2021) contempla, expresa y legalmente, las excepciones. Desde una perspectiva dogmática, los datos biométricos pueden entenderse como parte de la personalidad jurídica, tanto en su forma corporal como digital.

Representan un punto de conexión entre el cuerpo físico y la identidad jurídica, y su tratamiento implica una forma de mediación entre el ser humano y los sistemas de información. Por ello, la protección legal de estos datos no se limita a prevenir su uso comercial o fraudulento, sino

que abarca la defensa de la dignidad humana frente a la reducción de las personas a patrones biométricos cuantificables y explotables (Cuomo, 2015).

1.6. Obligaciones del empleador como responsable del tratamiento de datos biométricos frente a la finalidad y protección de los mismos

En el contexto de las relaciones laborales, el empleador que decide implementar sistemas de control de asistencia basados en tecnologías biométricas adquiere, en su calidad de responsable del tratamiento de datos personales, una serie de obligaciones legales y constitucionales cuyo cumplimiento es indispensable para garantizar el respeto a los derechos fundamentales del trabajador. Estas obligaciones se derivan, en primer lugar, del principio de legalidad en la Constitución de la República del Ecuador, y se desarrollan específicamente en la Ley Orgánica de Protección de Datos Personales, cuerpo normativo que impone un conjunto de deberes a quienes recolectan, almacenan, procesan o transmiten datos personales, y especialmente aquellos que pertenecen a la categoría de datos sensibles, como es el caso de los biométricos.

El artículo 10 de la Ley Orgánica de Protección de Datos Personales establece los principios rectores que guían todo tratamiento de datos personales. Entre ellos, destacan de forma particular la legalidad, la finalidad, la proporcionalidad, la pertinencia y minimización, y la confidencialidad. El empleador, en tanto responsable del tratamiento, está obligado a cumplir con cada uno de estos principios, tanto en el diseño del sistema de recolección de datos como en su implementación y posterior conservación. En primer lugar, la finalidad del tratamiento debe ser específica, explícita y legítima, conforme a lo señalado en la ley. En consecuencia, no se puede justificar la recolección de datos biométricos alegando finalidades genéricas como “mejorar el control de asistencia” si existen medios alternativos menos invasivos que permiten alcanzar el mismo propósito. Como señala Carrillo (2022) “*El principio de finalidad exige que los datos se utilicen únicamente para los fines expresamente autorizados, y que cualquier tratamiento extra o distinto requiera nuevo*

consentimiento del titular", constituye uno de los ejes centrales de la protección de datos personales. Este principio exige que toda recolección y tratamiento de datos responda a un fin legítimo, específico, expreso y conocido por el titular.

La determinación y justificación de la finalidad constituye una condición de licitud del tratamiento. El empleador debe demostrar que el uso de datos biométricos es estrictamente necesario para cumplir con una obligación legal o contractual. Debe garantizar que el uso de la proporcionalidad equilibre la violación de la dignidad del empleado con el valor de la eficiencia organizacional. El empleador debe justificar la proporcionalidad de la infracción determinando si los datos biométricos son el método más adecuado y menos intrusivo para lograr el objetivo establecido. La proporcionalidad limita el poder del empleador al garantizar la protección del principio de minimización de datos. El principio de minimización debe brindar confianza al empleador al establecer medidas organizativas, legales y administrativas para restringir el acceso no autorizado, la divulgación y el uso indebido de datos biométricos. Esa confianza debería extenderse a los procesadores de datos y a cualquier tercero que pueda acceder a ellos.

Es fundamental distinguir entre el «responsable del tratamiento» y el «encargado del tratamiento» de los datos. El «responsable del tratamiento» es la entidad que determina la finalidad y los medios del tratamiento de datos y, en última instancia, es responsable de la legalidad, la finalidad y la seguridad del mismo. Por el contrario, el «encargado del tratamiento» es la persona o entidad que trata los datos por cuenta del «responsable del tratamiento», siguiendo sus instrucciones y directrices, sin decidir la finalidad del tratamiento. Esta distinción es crucial para la asignación de obligaciones de cumplimiento y la consiguiente responsabilidad, ya que cada nivel es responsable de su propio conjunto de funciones y deberes en relación con el tratamiento de datos personales (Asamblea Nacional, 2023).

Como se indicó anteriormente, una de las obligaciones del empleador, en su calidad de responsable del tratamiento de datos, es justificar legalmente el uso de datos biométricos. De acuerdo con el artículo 26 de la Ley Orgánica de Protección de Datos de Carácter Personal, el tratamiento de datos sensibles está prohibido salvo que se aplique alguna excepción prevista por la ley, como el consentimiento explícito del interesado o el cumplimiento de una obligación legal o contractual.

El consentimiento del interesado es una de estas excepciones; sin embargo, como se ha argumentado en varias ocasiones, en el caso de una relación laboral, dicho consentimiento no puede considerarse libre, informado e inequívoco debido a la relación de subordinación que caracteriza este tipo de vínculo. García y López (2018) afirman: "*El consentimiento otorgado en relaciones de subordinación —como los contratos laborales— no puede considerarse pleno, por lo que el uso de datos sensibles requiere fundamentos jurídicos adicionales y una justificación objetivo*".

Desde otra perspectiva, cabe señalar que en Ecuador no existe ninguna normativa que obligue a los empleadores a utilizar sistemas biométricos para el control de asistencia. Por lo tanto, la obligación de tratar estos datos no se justifica por imperativo legal. Por tanto, sin base legal válida, el tratamiento de datos biométricos en el entorno laboral, aunque cuente con una declaración formal de consentimiento, podría ser considerado nulo por violación del principio de legalidad y del derecho a la autodeterminación informativa.

A ello se suma la obligación de realizar una evaluación de impacto en los casos en que el tratamiento implique un alto riesgo para los derechos y libertades de los titulares, tal como lo dispone el artículo 24 de la Ley Orgánica de Protección de Datos Personales. En el caso del uso de datos biométricos, donde se manipula información que no puede modificarse ni regenerarse, el riesgo es naturalmente alto y a evaluación

de impacto del tratamiento de datos personales es fundamental antes de implementar sistemas biométricos, especialmente en el ámbito laboral. El artículo 42 de la Ley Orgánica de Protección de Datos exige este análisis previo cuando hay riesgo «alto» para los derechos de los titulares, y la Superintendencia de Protección de Datos Personales ha señalado que sin dicha evaluación cualquier uso de biometría resulta jurídicamente imprudente (Asamblea Nacional, 2021; Super Intendencia de Protección de Datos Personales, 2025).

De igual manera Según la Agencia Española de Protección de Datos, el tratamiento de datos biométricos, considerados datos sensibles según el artículo 9 del Reglamento General de Protección de Datos, está prohibido salvo que se cumpla alguna de las excepciones previstas. En el contexto laboral, la Agencia Española de Protección de Datos señala que el consentimiento del trabajador no puede ser considerado una base válida para levantar esta prohibición debido al desequilibrio inherente en la relación laboral. Esto implica que el consentimiento no es libre, informado e inequívoco, lo que lo hace inapropiado como fundamento jurídico para el tratamiento de datos biométricos en el ámbito laboral (Agencia Española de Protección de Datos, 2023)

1.7. Garantías legales del sujeto pasivo de datos biométricos frente a la realidad en el Ecuador

El ordenamiento jurídico ecuatoriano reconoce expresamente un conjunto de garantías legales para la protección del titular de datos personales, en especial cuando se trata de los datos biométricos. Su efectividad depende no solo de su consagración normativa, sino también de su implementación adecuada, supervisión institucional y posibilidad real de exigencia por parte de los titulares. En la práctica ecuatoriana, persiste una brecha considerable entre la garantía formal de derechos y la realidad del ejercicio pleno de los mismos, especialmente en contextos de relaciones asimétricas como las laborales.

Esta norma constitucional se proyecta como una garantía directa, que protege la esfera íntima del individuo frente al poder público y privado, estableciendo límites al tratamiento automatizado y masivo de información personal. Además, como lo señala la Corte Constitucional en la Sentencia No. 2064-14-EP/21, "*El consentimiento […] requiere ser libre, específica, informada e inequívoca. Libre implica que no esté sujeto a vicio por fuerza, coerción o presión… informada implica conocer a detalle el uso que se va a dar al dato personal, además de conocer la finalidad […]*", lo cual adquiere especial relevancia en el tratamiento de datos biométricos en entornos laborales.

La Ley Orgánica de Protección de Datos Personales refuerza este marco constitucional a través de un sistema normativo específico de garantías orientado a salvaguardar la autonomía informativa del titular. Entre los derechos que reconoce la ley destacan: el derecho al acceso (art. 13), rectificación y actualización (art. 14), eliminación (art. 15), oposición (art. 16), portabilidad (art. 17), suspensión del tratamiento (art. 19) y el derecho a no ser objeto de decisiones automatizadas (art. 20). Estas garantías son exigibles tanto frente a entidades públicas como privadas. Asimismo, la Superintendencia de Protección de Datos Personales actúa como autoridad de control y supervisión, encargada de prevenir, investigar y sancionar infracciones a la normativa vigente.

Sin embargo, a pesar de este marco legal robusto, la realidad ecuatoriana demuestra limitaciones estructurales en la aplicación efectiva de estas garantías. En primer lugar, la asimetría de poder entre los responsables del tratamiento (empleadores, entidades estatales, corporaciones) y los titulares (ciudadanos, trabajadores, usuarios) limita el ejercicio voluntario y efectivo de los derechos. "*Los derechos humanos no se realizan simplemente por su proclamación, sino cuando existen condiciones efectivas – institucionales, materiales y culturales – que permiten su ejercicio y exigibilidad*" (Rodríguez López, 2020). En el caso de los trabajadores, el temor a represalias, la falta de conocimiento

jurídico y la debilidad institucional dificultan el ejercicio del derecho a negarse al tratamiento de sus datos biométricos sin consecuencias laborales.

Además, en la práctica, los procedimientos para ejercer los derechos de protección de datos personales no se encuentran del todo consolidados ni accesibles. Si bien la Ley Orgánica de Protección de Datos Personales establece la obligación de crear medios precisos y eficaces para el ejercicio de los derechos de acceso, supresión y revocación del consentimiento, la mayoría de las entidades aún no han podido establecer oficinas, protocolos internos y recursos humanos adecuados para el cumplimiento de dichas solicitudes. Esto genera una desprotección estructural, que convierte los derechos en normas meramente declarativas en lugar de mecanismos exigibles y efectivos (Super Intendencia de Protección de Datos Personales, 2025).

La Superintendencia de Protección de Datos Personales, creada formalmente en 2023 y conforme a lo previsto por la ley, se encuentra aún en fase de desarrollo institucional, lo que limita considerablemente su capacidad de supervisión, prevención y sanción de conductas sujetas a regulación. La falta de registros administrativos y de jurisprudencia en el tema, sumada a una cultura de protección de datos poco desarrollada, hace difícil la creación de un contexto en el que el cumplimiento de la normativa sea proactivo y eficaz.

Asimismo, las limitaciones descritas anteriormente se ven agravadas por el desconocimiento general de la población respecto al alcance y los mecanismos de protección de datos personales. Este desconocimiento general, que, junto con una falta de conciencia sobre la privacidad y la seguridad de los datos, socava profundamente las perspectivas de implementar medidas de protección significativas para los individuos dentro de un país. Tal ignorancia socava el ejercicio de los derechos de oposición, revocación del consentimiento y eliminación de datos, especialmente cuando los datos se procesan bajo justificaciones vagas y

mecanismos coercitivos indirectos. Para que el derecho a la protección de datos sea significativo, requiere leyes claras y una población que comprenda y esté activa; de lo contrario, el derecho se vuelve inútil.

A pesar de que Ecuador cuenta con marcos legales coherentes y apropiados para proteger los datos personales y biométricos, aún existen importantes desafíos para hacer efectivas las garantías para el sujeto pasivo. Para culminar la consolidación institucional, la construcción de mecanismos transparentes, la capacitación de los agentes responsables y la educación del público son los elementos clave para cerrar la brecha entre el derecho proclamado y el ejercido (Superintendencia de Protección de Datos Personales, 2025). Hasta que esto ocurra, el tratamiento de datos biométricos, particularmente en el lugar de trabajo, seguirá siendo un tema controvertido en la defensa de los derechos digitales.

El estudio de los datos biométricos bajo la Ley Orgánica de Protección de Datos Personales y el principio de legalidad indica que Ecuador ha avanzado en la construcción de un marco jurídico donde la protección de datos es un derecho fundamental. Sin embargo, esto no ha sido del todo efectivo. En particular, se cuestiona la legalidad, la necesidad y la proporcionalidad del control biométrico por parte del empleador en el trabajo, así como la protección del derecho del trabajador al uso de la tecnología biométrica. La consolidación de un sistema de protección de datos que aborde la dignidad del trabajo, como señala González Fuster, requiere la correcta aplicación de los principios de la Ley Orgánica de Protección de Datos Personales, el cumplimiento de la responsabilidad del control de datos, el fortalecimiento institucional de las garantías y la dignidad del trabajo. Los sistemas jurídicos de protección de datos, especialmente para los sistemas biométricos, donde reside la dignidad y la autonomía del trabajador, deben ser efectivos y aplicables, no solo existir formalmente (González Fuster, 2014; Asamblea Nacional, 2021).

Capitulo II
Derecho Comparado de la Normativa Ecuatoriana con el Marco Jurídico Internacional, que Regulan el Uso de Datos Biométricos en Entornos Laborales.

2.1. Normativa ecuatoriana aplicable al uso de datos biométricos en entornos laborales

El consentimiento para el tratamiento de datos biométricos debe cumplir con condiciones de validez sustanciales: ser libre, específico, informado e inequívoco. En relaciones laborales, donde existe una relación de subordinación y un posible temor reverencial hacia el empleador, esta libertad puede verse comprometida. Tal como lo señala el Comité Europeo de Protección de Datos (2011), el consentimiento en contextos de subordinación, como la relación laboral, puede no considerarse libre, por lo que debe ser evaluado con estrictos criterios de legalidad y proporcionalidad.

Adicionalmente, la Ley Orgánica de Protección de Datos Personales obliga al empleador, en calidad de responsable del tratamiento, a respetar principios fundamentales como la finalidad, la proporcionalidad, la minimización de datos, la seguridad y la confidencialidad. En caso de que el tratamiento de datos biométricos no sea estrictamente necesario para la finalidad laboral específica y existan otros medios menos invasivos para lograrla como tarjetas magnéticas, códigos o registros manuales, la práctica puede resultar desproporcionada y, por tanto, contraria al principio de legalidad.

La normativa también exige la realización de evaluaciones de impacto de protección de datos cuando el tratamiento implique alto riesgo para los derechos de los titulares, obligación que aplica especialmente en el uso de tecnología biométrica. Esta medida tiene como finalidad anticipar riesgos y mitigar posibles afectaciones a los derechos fundamentales de los trabajadores (Agencia Española de Protección de Datos, 2022).

La legislación ecuatoriana establece un marco robusto para la protección de datos biométricos en entornos laborales, pero su aplicación práctica depende del cumplimiento estricto de los principios y requisitos legales, siendo fundamental evitar cualquier forma de coacción o imposición que pudiera viciar el consentimiento o transgredir derechos fundamentales (Rosas, G & Cardenas, G, 2023).

2.2. Comparación entre la Ley Orgánica de Protección de Datos Personales del Ecuador y la Ley N.º 21719 Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador y la Ley N.º 21719 Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales constituyen los marcos jurídicos nacionales destinados a regular el tratamiento de datos personales. Ambas normas comparten el objetivo de salvaguardar la privacidad de los individuos, aunque difieren sustancialmente en su estructura, alcance y grado de actualización. La Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021) reconoce explícitamente los datos biométricos como datos personales sensibles y establece un régimen especial de protección que prohíbe su tratamiento salvo excepciones previstas en la ley.

El tratamiento de datos personales en entornos laborales se encuentra regulado por marcos legales nacionales que buscan garantizar

la protección de la privacidad y los derechos fundamentales de los individuos. En este sentido, la Ley Orgánica de Protección de Datos Personales del Ecuador y la Ley N.º 21.719 de Chile, que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales, constituyen referentes normativos clave en sus respectivos países. Aunque ambas normas persiguen objetivos similares, presentan diferencias importantes en cuanto a estructura, alcance y aplicación práctica, especialmente en lo que respecta al tratamiento de datos sensibles como los biométricos.

La Ley Orgánica de Protección de Datos Personales ecuatoriana (Asamblea Nacional, 2021) reconoce explícitamente los datos biométricos como datos personales sensibles y establece un régimen especial de protección que prohíbe su tratamiento salvo en los casos excepcionales contemplados en la ley, tales como el consentimiento libre, informado e inequívoco del titular, o la existencia de una obligación legal o contractual que justifique su uso. La normativa analizada establece principios que deben seguirse, entre los que se incluyen la finalidad, la proporcionalidad, la minimización de datos, la seguridad, la confidencialidad y la evaluación de riesgos relacionados con la protección de datos, así como las evaluaciones de impacto de la protección siempre que el tratamiento de datos implique altos riesgos para los derechos de los interesados.

Además, la Ley chilena N° 21.719 (2022) regula el tratamiento de datos personales sensibles y establece que dicho tratamiento debe basarse en el consentimiento del titular o en otros fundamentos jurídicos, como el cumplimiento de obligaciones legales o la ejecución de contratos. Esta ley también creó la Agencia de Protección de Datos Personales, que realiza funciones de auditoría y vela por el cumplimiento de la ley, y estableció mecanismos de control y sanción para el tratamiento ilícito de datos personales. Sin embargo, la legislación chilena ofrece un enfoque mucho menos integral para la regulación del tratamiento de datos biométricos en las relaciones laborales. Se limita a establecer principios generales de protección y seguridad.

Una diferencia significativa entre ambas normativas radica en la distinción entre el «responsable del tratamiento» y el «encargado del tratamiento», claramente definida en la Ley Orgánica de Protección de Datos Personales de Ecuador. Esta diferencia es relevante en el ámbito laboral, ya que aclara las obligaciones y responsabilidades legales de las entidades que tratan datos biométricos al determinar los fines del tratamiento y de aquellas que simplemente actúan por delegación. La legislación chilena, en cambio, se refiere principalmente al «responsable del tratamiento» y no profundiza en el concepto de «encargado del tratamiento».

Ambas leyes, fieles al espíritu de protección de los derechos del titular de los datos, le otorgan los derechos de acceso, rectificación, supresión, oposición y portabilidad de sus datos personales. Sin embargo, la experiencia práctica en Ecuador demuestra que los medios prácticos para ejercer estos derechos no están plenamente consolidados ni son fácilmente accesibles, lo que genera una brecha entre la ley y su aplicación efectiva. Esta brecha evidencia la necesidad de una supervisión activa por parte de la Superintendencia de Protección de Datos Personales de Ecuador y la Agencia de Protección de Datos de Chile.

Instituciones encargadas del control

Estas regulaciones se cumplen gracias a la existencia de organismos reguladores que supervisan y controlan el manejo adecuado de los datos personales:

Ecuador: Superintendencia de Protección de Datos Personales (SPDP):

La Superintendencia de Protección de Datos Personales de Ecuador es la autoridad en territorio ecuatoriano que promueve, regula y supervisa el tratamiento de datos personales. Supervisa el cumplimiento de la Ley Orgánica de Protección de Datos Personales, la emisión de

directrices y resoluciones, la atención de consultas y quejas de los titulares de los datos y la imposición de sanciones por infracciones. Esta institución es fundamental para garantizar que la biometría y la protección de datos en el ámbito laboral se rijan por los principios de legalidad, proporcionalidad y seguridad (Superintendencia de Protección de Datos Personales, 2025).

Chile: Agencia de Protección de Datos Personales:

La Agencia chilena es una corporación autónoma de derecho público cuyo objetivo es la protección de los derechos de datos personales de la persona. Entre sus funciones se encuentran la supervisión del cumplimiento de la Ley N° 21.719, la emisión de normas generales de protección de datos, la vigilancia de las infracciones, la aplicación de sanciones y la promoción de la educación en materia de protección de datos.Esta institución actúa como garante de que los responsables del tratamiento implementen medidas adecuadas de seguridad y respeten los derechos de los titulares (Ley N.º 21.719, 2022).

2.3. Comparación de la Ley Orgánica de Protección de Datos Personales y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea

La Ley Orgánica de Protección de Datos Personales de Ecuador y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea constituyen dos marcos legales en materia de protección de datos personales. Ambas normativas abordan la protección de datos personales sensibles, incluidos los datos biométricos. La Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021, art. 4) y el RGPD (Parlamento y Consejo de Europa, 2016, art. 9) establecen que el tratamiento de este tipo de datos está prohibido, salvo excepciones específicas previstas en la ley. En consecuencia, el uso de datos biométricos está sujeto a requisitos legales reforzados, entre los que se

incluyen la necesidad de contar con una finalidad legítima, una evaluación de riesgos y medidas de seguridad técnicas y organizativas adecuadas.

El Reglamento General de Protección de Datos de la Unión Europea (RGPD) es un punto de referencia internacional para un marco legal completo y exhaustivo que trata sobre la privacidad y los datos personales, así como los derechos y leyes fundamentales de la UE (Rocío Albert López-Ibor, 2019). En un contexto legal y socioeconómico completamente diferente, mientras que la Ley Orgánica de Protección de Datos Personales es un importante reconocimiento de las de protección que Ecuador ha implementado para la privacidad de los datos personales de sus ciudadanos, tiene divergencias diferentes y, en algunos aspectos, más significativas en comparación con el modelo europeo.

Aunque ambas normativas comparten los mismos principios fundamentales, como legalidad, finalidad, proporcionalidad, calidad, transparencia y responsabilidad en relación con los datos personales, el Reglamento General de Protección de Datos (GDPR) tiene una estructura más elaborada y un marco regulatorio más amplio enfocado en los desafíos planteados por la globalización digital y el marco regulatorio desigual de los estados miembros. Un claro ejemplo de la diferencia en el enfoque es la inclusión por el RGPD (Parlamento Europeo y Consejo) de los principios de 'privacidad por diseño' y 'privacidad por defecto', que requieren que los responsables del tratamiento implementen medidas de protección durante las etapas iniciales del procesamiento de datos y aseguren que la configuración predeterminada sea la más protectora. Estos conceptos no se desarrollan de manera explícita en la Ley Orgánica de Protección de Datos Personales de Ecuador (Agencia Española de Protección de Datos, 2019).

Con respecto a la aplicación de la ley, el Reglamento General de Protección de Datos tiene un alcance extraterritorial efectivo y se aplica a cualquier entidad, independientemente de su ubicación geográfica, que

procese los datos personales de individuos ubicados en la Unión Europea.

Esta característica es esencial para afrontar los retos que plantea la globalización del tratamiento de datos y el comercio electrónico. La Ley Orgánica de Protección de Datos Personales, en cambio, tiene un enfoque territorial más limitado, centrado en la protección de las personas dentro del territorio nacional, lo que puede resultar menos eficaz en escenarios de tratamiento transfronterizo de datos, bastante común hoy en día (Kuner, 2017).

Por lo tanto, la divergencia entre ambas leyes se explica por los entornos económicos y digitales particulares en los que se desarrollaron, así como por las prioridades de política pública de las respectivas jurisdicciones. Mientras que el Reglamento General de Protección de Datos (RGPD) responde a un mercado digital globalmente integrado que exige un régimen de protección unificado para los derechos individuales, la Ley Orgánica de Protección de Datos se centra en el contexto nacional, ya que busca garantizar el derecho a la privacidad y la seguridad de los datos, reflejando así la capacidad regulatoria del país. La necesidad de proteger los datos personales es común a ambos marcos legales; sin embargo, su aplicabilidad internacional es limitada y seguirá siéndolo, en gran medida, debido al alcance explícito de cada marco legal y a la capacidad de las autoridades de control para garantizar su cumplimiento.

Desde el enfoque de las posibles sanciones, el Reglamento General de Protección de Datos (RGPD) contempla, en su artículo 83, multas administrativas de hasta 20 millones de euros o el 4% de la cifra de negocio anual total, eligiendo la cantidad mayor. Estas sanciones buscan el estricto cumplimiento del reglamento y actúan como elemento disuasorio (Cabezas, M. y Lucas, G., 2024). A diferencia de la Ley Orgánica de Protección de Datos Personales, estos recursos financieros pueden generar una disuasión efectiva. Esto se combina con una cultura

de cumplimiento dentro de las organizaciones y la cultura de riesgo que estas mismas organizaciones tienen en Ecuador.

El Reglamento General de Protección de Datos (RGPD) establece un marco institucional centrado en la cooperación y la coherencia entre las Autoridades de Protección de Datos de los Estados miembros, particularmente en el marco del propio Reglamento. Este marco institucional fomenta la certeza jurídica y una respuesta efectiva a las violaciones transfronterizas de derechos. En el ámbito de la Ley Orgánica de Protección de Datos Personales de los Ciudadanos Ecuatorianos, Ecuador no puede desarrollar estas potencialidades, que en el artículo 53, sección f, prevé la creación de un Oficial de Protección de Datos para supervisar y hacer cumplir el cumplimiento. No existen bases en la región ni en el sistema internacional para el seguimiento y la cooperación en el tratamiento de datos personales en el contexto internacional (Cabezas, M. y Lucas, G., 2024).

Entre los 'datos especialmente sensibles', la importancia del procesamiento de datos biométricos tiene prioridad. Estos datos son sensibles por naturaleza y, por lo tanto, su procesamiento y salvaguarda requieren precauciones extraordinarias. La legislación de la UE designa estos datos como 'especialmente' sensibles y requiere el consentimiento explícito e informado de los interesados, excepto en casos de obligación legal, protección de la vida de la persona o interés público significativo. La legislación sobre datos biométricos enfatiza particularmente las restricciones, ya que estos datos son identificables y presentan riesgos de uso indebido o abuso. McCormack y Achuthan (2022) señalan que la Ley Orgánica de Protección de Datos Personales de Ecuador reconoce la disposición protectora especial de los datos sensibles, pero no ofrece regulaciones sectoriales desarrolladas con el mismo nivel de detalle. Esto puede dejar una interpretación excesiva y potencialmente peligrosa en la práctica, como señala Pérez Asinari (2022).

El Reglamento General de Protección de Datos establece cuatro elementos clave como criterios para el Consentimiento: "incondicionado, explícito, informado y revocable en cualquier momento, y evidenciado por el interesado". En el caso de relaciones laborales donde existe una posición subordinada, Voigt & Von dem Bussche (2017) afirman que la regulación europea proporciona un medio para evaluar la validez del consentimiento, y el uso del consentimiento como base legal para el procesamiento está limitado dentro de las relaciones de desequilibrio de poder, en las que otros fundamentos legales como la obligación legal y el interés legítimo son priorizados.

Aunque la Ley Orgánica de protección de datos requiere que se otorgue consentimiento para el procesamiento de datos personales, aún no existen, sin embargo, estándares legales específicos para la validez del consentimiento en relaciones laborales subordinadas, lo que dificulta prácticamente la protección del empleado frente al posible riesgo de presión indebida.

El Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD), especifica, en virtud del principio de subsidiariedad y responsabilidad, que quienes tratan datos deben garantizar y demostrar el cumplimiento mediante la adopción de medidas técnicas y organizativas adecuadas, lo que incluye el mantenimiento de registros de actividad, la realización de evaluaciones de impacto relativas a la protección de datos y el respeto de los plazos obligatorios para la notificación de brechas de seguridad. Esta obligación fomentará una cultura de prevención y cumplimiento que facilitará el tratamiento de datos de forma transparente y segura. La Ley Orgánica de Protección de Datos, por otro lado, también asigna responsabilidad al responsable del tratamiento e impone la obligación de adoptar medidas de seguridad, pero, en lo que respecta a las evaluaciones de impacto, resulta insuficiente en especificidad y detalle, lo que a su vez limita las consecuencias del fortalecimiento de la prevención y el control de riesgos (Cabezas, M. y Lucas, G., 2024).

Las autoridades tienen la facultad de realizar auditorías, implementar medidas correctivas e iniciar procedimientos legales. En Ecuador, la Ley de Protección de Datos Personales crea una única autoridad para la protección de datos personales, pero con facultades, recursos y autonomía operativa limitados. Por lo tanto, no se alcanza la independencia y capacidad de intervención previstas en el modelo europeo, lo que puede afectar la eficacia del sistema nacional en materia de violaciones e infracciones (Kuner, 2017).

En cuanto al proceso de armonización y alineación con el contexto internacional, el Reglamento General de Protección de Datos (RGPD) ha tenido un impacto decisivo en la creación de normativas en diversas jurisdicciones, estableciendo estándares mínimos comunes y permitiendo la interoperabilidad normativa. La Ley de Protección de Datos Personales busca cumplir con estos estándares internacionales, pero cuestiones estructurales impiden la armonización normativa total, particularmente en lo que respecta a la falta de acuerdos específicos de transferencia de datos y medidas de protección de datos transfronterizas aprobadas por la UE, elementos clave en la colaboración internacional en materia de protección de datos (Comité Europeo de Protección de Datos, 2021).

La comparación entre la Ley Orgánica de Protección de Datos Personales ecuatoriana y el Reglamento General de Protección de Datos europeo evidencia que, aunque comparten fundamentos y objetivos comunes, el marco europeo se distingue por una mayor profundidad normativa, alcance extraterritorial, robustez sancionadora y estructura institucional que garantizan una protección más integral y adaptada a la complejidad del entorno digital actual.

2.4. Estándares de la Organización para la Cooperación y el Desarrollo Económicos y otras recomendaciones internacionales

En el análisis del marco normativo internacional que regula la protección de datos personales, la Organización para la Cooperación y el

Desarrollo Económicos (OCDE) ocupa un lugar preponderante como uno de los primeros organismos en establecer estándares y principios orientadores para la gestión responsable de la información personal. Desde la publicación de sus primeras directrices en 1980, la Organización para la Cooperación y el Desarrollo Económicos ha promovido principios básicos que han influenciado notablemente el diseño de legislaciones nacionales y regionales en materia de privacidad y protección de datos, incluyendo la Ley Orgánica de Protección de Datos Personales del Ecuador y el Reglamento General de Protección de Datos de la Unión Europea (Organización para la Cooperación y el Desarrollo Económicos, 2013).

La OCDE ha desarrollado principios que se agrupan en sus Directrices en materia de protección de la privacidad y de las transferencias de datos personales en el ámbito internacional. Estos son: restricción de la recopilación, calidad de los datos, finalidad, limitación del uso, seguridad, apertura y transparencia, participación y rendición de cuentas. Estos principios buscan garantizar el equilibrio entre la circulación de información para el desarrollo de actividades económicas y la protección de los derechos fundamentales, en particular el derecho de las personas a la privacidad (Organización para la Cooperación y el Desarrollo Económicos, 2013).

La Organización para la Cooperación y el Desarrollo Económicos también ha señalado la importancia de la colaboración internacional para abordar los desafíos del flujo transfronterizo de datos y ha enfatizado la necesidad de establecer mecanismos que garanticen un nivel adecuado de protección, independientemente del país en el que se realice el procesamiento de datos.

Aquí, la cooperación se entiende como la presentación de propuestas para desarrollar marcos legales compatibles, crear mecanismos de supervisión efectivos y establecer acuerdos bilaterales o multilaterales que faciliten la protección y el intercambio seguro de

información (Organización para la Cooperación y el Desarrollo Económico, 2013).

Sin embargo, la Organización para la Cooperación y el Desarrollo Económico (OCDE) no es la única entidad internacional involucrada en la cooperación. Por ejemplo, el Consejo de Europa, a través de la Convención 108 sobre la protección de individuos en relación con el procesamiento automático de datos personales, proporcionó un instrumento legal vinculante que permite la armonización de las leyes internacionales de protección de datos y establece estándares mínimos en la protección de datos personales con énfasis en la salvaguarda de derechos y el control estatal (Consejo de Europa, 1981). Esta convención fue revisada y actualizada en 2018 para incluir, entre otras cosas, el procesamiento de datos biométricos y genéticos, fortaleciendo la protección en el lugar de trabajo y otras áreas críticas.

Además, las directrices y recomendaciones de la Comisión Interamericana de Derechos Humanos y de las Naciones Unidas ayudan a formar parte del consenso internacional sobre la protección de datos personales y los aspectos humanitarios de los derechos internacionales. La Comisión Interamericana de Derechos Humanos formuló principios sobre la protección de datos personales y la privacidad que subrayan la importancia de la seguridad y la confidencialidad, el consentimiento informado, la minimización de datos y la protección y confidencialidad de la privacidad. Estos principios discuten la importancia de la protección y la confidencialidad de la privacidad, particularmente cuando se trata de datos biométricos en el contexto laboral (Comisión Interamericana de Derechos Humanos, 2017).

Con respecto a la Incorporación de Normas Internacionales, el Reglamento de Protección de Datos de Ecuador buscará similar estos principios dentro del ámbito del Reglamento Ecuatoriano de Protección de Datos para garantizar una protección más efectiva de los derechos de los titulares de datos, permitiendo así que Ecuador participe plenamente en el

panorama económico y tecnológico global. Ecuador proporcionará mayor seguridad a la ciudadanía y a los socios internacionales sobre la creación de canales de comunicación seguros, el intercambio de datos privados confidenciales y la protección de la confidencialidad de los datos. Esto facilitará la comunicación y la transferencia segura de datos, mientras se protege la privacidad de los datos para las partes principales.

Las normas de la OCDE se destacan sobre todo por la importancia que otorgan a la autorregulación responsable por parte del sector privado y la construcción de un entorno de confianza digital. Si bien estos principios no poseen fuerza legal vinculante por sí solos, su adopción en diferentes jurisdicciones ha ayudado a consolidar una base común a partir de la cual se desarrollan los regímenes nacionales, incluido el ecuatoriano. En este contexto, la Ley Orgánica de Protección de Datos Personales del Ecuador, en varios de sus artículos, parece incorporar los lineamientos de la OCDE, particularmente con relación a los principios de limitación de finalidad, calidad de los datos y las obligaciones de los responsables del tratamiento. Sin embargo, aún se evidencian vacíos normativos en cuanto a la implementación de sistemas eficaces de rendición de cuentas y mecanismos de supervisión técnica y ética que garanticen el cumplimiento efectivo de estos principios en contextos prácticos como el laboral (Organización para la Cooperación y el Desarrollo Económicos, 2013; Greenleaf, 2014).

Es importante mencionar el creciente reconocimiento, dentro del ámbito de la regulación, de la protección de datos personales como un componente del marco de derechos humanos, y no únicamente como un derecho técnico. En este sentido, las Directrices sobre Inteligencia Artificial y Protección de Datos del Consejo de Europa, publicadas en 2020, abogan por una regulación que reconozca la naturaleza intrusiva, particularmente en las relaciones laborales, de ciertas tecnologías, como los sistemas de identificación biométrica. Estas recomendaciones destacan la importancia de los derechos fundamentales en la evaluación de tecnologías de control o vigilancia y la urgente necesidad de que

países como Ecuador articulen legislativamente el imperativo de las evaluaciones de impacto y el establecimiento de límites y protecciones legales en el manejo de datos sensibles.

En el contexto interamericano, el Relator Especial sobre la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos 2021, también ha señalado la importancia de la legalidad, necesidad y proporcionalidad en el uso de tecnologías de reconocimiento y verificación biométrica en el lugar de trabajo. También ha destacado el potencial de estas tecnologías para infringir los derechos a la libertad, especialmente la autonomía y la privacidad, cuando se instalan dispositivos de control y vigilancia para captar la atención de los trabajadores fuera de las horas laborales, y cuando se establece una vigilancia continua sin la debida justificación legal. Estos comentarios son especialmente importantes para Ecuador como resultado de asimetrías de poder, el incumplimiento de los privilegios en los sectores más explotados de cumplir con los marcos legales, y las debilidades en curso en los marcos institucionales del país.

La Declaración Conjunta sobre Libertad de Expresión y Privacidad (2018), firmada por relatores internacionales de la ONU, la OEA y otras entidades regionales, establece principios orientadores para garantizar que las medidas tecnológicas implementadas por actores públicos o privados respeten el derecho a la privacidad. En dicho documento se insta a los Estados a promulgar leyes claras, proporcionales y transparentes que regulen el tratamiento de datos personales, especialmente en escenarios donde existe asimetría de poder, como el que se da entre empleador y trabajador. Ecuador, si bien ha dado pasos relevantes al promulgar la Ley Orgánica de Protección de Datos, aún se encuentra en una etapa incipiente de implementación y armonización con este tipo de recomendaciones, particularmente en lo que respecta a la fiscalización efectiva del uso de tecnologías biométricas por parte de entidades privadas (ONU, OEA, OSCE & CADHP, 2018).

Cabe mencionar que la tendencia internacional apunta a la consolidación de un estándar global que supere la mera protección formal de datos personales y transite hacia un enfoque basado en el riesgo y los derechos fundamentales. Esta perspectiva demanda una comprensión crítica del impacto estructural que tienen ciertas tecnologías sobre colectivos vulnerables. En consecuencia, el tema del procesamiento de datos biométricos en el lugar de trabajo va más allá del cumplimiento legal y toca la ética y gobernanza de la institución. La alineación de Ecuador con estos estándares internacionales significa más que los ajustes normativos de la Ley Orgánica de Protección de Datos; requiere el establecimiento de capacidades institucionales, técnicas y humanas apropiadas para asegurar que las condiciones laborales protejan la dignidad del trabajador frente al procesamiento indiscriminado y automatizado de sus datos personales más sensibles (Consejo de Europa, 2018; OCDE, 2013; ONU, 2021).

Los estándares y recomendaciones internacionales emanados de la Organización para la Cooperación y el Desarrollo Económicos y otros organismos relevantes constituyen pilares fundamentales para la protección de datos personales en la era digital. Su incorporación en la legislación nacional, como en el caso de la Ley Orgánica de Protección de Datos, resulta esencial para desarrollar un régimen jurídico robusto, coherente y compatible con las mejores prácticas globales, particularmente en el tratamiento de datos sensibles y biométricos en entornos laborales.

2.5. Valoración del grado de armonización normativa de Ecuador con estándares internacionales

La valoración del grado de armonización normativa entre el marco ecuatoriano de protección de datos personales y los estándares internacionales constituye un ejercicio fundamental para medir la madurez y efectividad del sistema jurídico nacional frente a los retos de la gobernanza digital. En este contexto, la promulgación de la Ley Orgánica de Protección de Datos Personales en el año 2021, realizo un avance

normativo significativo en Ecuador, al reconocer el derecho a la protección de datos personales como un derecho autónomo, con base constitucional y sujeto a garantías jurídicas específicas.

No obstante, a pesar de su existencia formal, su alineación sustantiva con instrumentos internacionales como el Reglamento General de Protección de Datos, las Directrices de la Organización para la Cooperación y el Desarrollo Económicos, el Convenio 108+ del Consejo de Europa y los pronunciamientos de la Comisión Interamericana de Derechos Humanos (CIDH), aún presenta inconsistencias, omisiones y debilidades estructurales que deben ser evaluadas de manera crítica. Estas inconsistencias se manifiestan principalmente en la cobertura de derechos y principios, donde algunos derechos de los titulares no están plenamente garantizados o carecen de procedimientos claros para su ejercicio efectivo, incluyendo aspectos como el acceso, rectificación, supresión, oposición, portabilidad y el derecho al olvido, así como la aplicación de principios fundamentales como la minimización de datos y la privacidad desde el diseño Consejo de Europa, 2018; Comisión Interamericana de Derechos, 2014).

Desde una perspectiva formal, la Ley Orgánica de Protección de Datos Personales ecuatoriana adopta principios rectores coherentes con los estándares internacionales: legalidad, finalidad, proporcionalidad, minimización de datos, calidad, transparencia, seguridad, responsabilidad y confidencialidad.

Esta convergencia se hace evidente en el conjunto de normas y en el diseño general relativo al reconocimiento de los derechos de los interesados, así como al reconocimiento de los derechos de acceso, rectificación, supresión, oposición y portabilidad. Sin embargo, al valorar el grado de armonización desde una dimensión sustantiva y operativa, se advierte que la implementación práctica de estos principios no siempre garantiza su eficacia jurídica ni su equivalencia funcional con las normas europeas o con las recomendaciones de la Organización para la

Cooperación y el Desarrollo Económicos (International Association of Privacy Professionals, 2023).

Un ejemplo claro de esta diferencia se encuentra en la figura del consentimiento. Si bien la Ley Orgánica de Protección de Datos Personales exige consentimiento para el tratamiento de datos personales y especialmente para los datos biométricos, no incorpora una regulación específica para contextos de desequilibrio de poder, como las relaciones laborales, en las que el consentimiento del trabajador puede no ser libre. En contraste, el Reglamento General de Protección de Datos, las Directrices de la Organización para la Cooperación y el Desarrollo Económicos y los pronunciamientos de organismos interamericanos recalcan que en entornos donde existe subordinación, el consentimiento no debe ser la base jurídica preferente, recomendándose otras como la obligación legal o el interés público legítimo. Esta ausencia de una regulación diferenciada en el contexto ecuatoriano limita su capacidad de alinearse con la doctrina internacional más garantista (Comisión Interamericana de Derechos, 2017; Voigt & Von dem Bussche, 2017).

Otro aspecto que evidencia una armonización parcial es el relativo a la figura de la Evaluación de Impacto en la Protección de Datos (DPIA, por sus siglas en inglés: Data Protection Impact Assessment). El Reglamento General de Protección de Datos establece la obligatoriedad de estas evaluaciones cuando el tratamiento pueda implicar un alto riesgo para los derechos y libertades de las personas físicas, como ocurre con tecnologías biométricas utilizadas en el ámbito laboral. Al igual que en el caso anterior, la Ley Orgánica de Protección de Datos de Ecuador y su Reglamento contemplan la realización de evaluaciones de impacto y especifican su alcance, carácter obligatorio, metodología y componentes, como la descripción de las operaciones de tratamiento y la identificación de riesgos (Asamblea Nacional, 2021; 2023). Sin embargo, en comparación con el Reglamento General de Protección de Datos (RGPD), la profundidad y el detalle de los procedimientos siguen siendo insuficientes, particularmente en lo que respecta a la supervisión activa

del responsable del tratamiento, lo que sugiere la necesidad de una mayor capacidad institucional para monitorear los derechos de los titulares de los datos mediante la vigilancia proactiva y la protección de sus derechos.

Además, el grado de articulación de Ecuador con instrumentos internacionales, como el Convenio 108 del Consejo de Europa, aún se encuentra en una fase incipiente. Si bien Ecuador puede adoptar este instrumento, no ha iniciado el proceso de adhesión formal. Esto representa una oportunidad normativa para que Ecuador no solo mejore su alineación con los estándares globales, sino que también fortalezca la cooperación internacional y obtenga el reconocimiento de adecuación con respecto al flujo transfronterizo de datos personales, promoviendo así la transferencia internacional segura de datos (GADISA, 2023).

Cabe mencionar la integración gradual de Ecuador con el Convenio 108 de la Unión Europea y el Reglamento GADISA Vertical de 2023. Ecuador podría adoptar el instrumento, pero aún no ha iniciado el proceso de adhesión. Esto no implica que no existan perspectivas positivas para la legislación ecuatoriana. Ecuador podría intensificar sus esfuerzos de armonización legal con los estándares internacionales y el reconocimiento en la cooperación internacional, la transferencia internacional legal, segura y protegida de datos personales, el registro de datos personales y el marco internacional de regulación de datos. Igualmente importante es reconocer la necesidad de una política pública nacional sólida en materia de protección de datos, junto con estrategias de capacitación, veto y sensibilización para los sectores público y privado, diseñadas para la supervisión. La armonización normativa legal no se limita ni se logra con un texto promulgado; también requiere condiciones institucionales, socioculturales y tecnoestructurales. En este sentido, Ecuador ha realizado importantes esfuerzos, especialmente en el manejo de datos biométricos y laborales, áreas que requieren una cultura organizacional sólida (Consejo de Europa, 2018).

En primer lugar, conviene señalar los problemas derivados de la armonización internacional y, a continuación, analizar la armonización interna, que en el caso que nos ocupa se refiere a la incorporación al ordenamiento jurídico ecuatoriano. Esto se debe a que, desde la perspectiva de la armonización normativa en la doctrina internacional, se busca la implementación a nivel internacional de diversas legislaciones, en este caso de la región andina. Esta ausencia puede generar lagunas legales e interpretativas, en particular con respecto a los sofisticados sistemas biométricos utilizados en los centros de trabajo. En este sentido, el grado de armonización se ve limitado no solo por la redacción de la ley, sino también por su escasa capacidad de respuesta ante la anticipación normativa derivada del rápido ritmo del desarrollo tecnológico (Comité Europeo de Protección de Datos, 2020).

Otro punto que limita la armonización efectiva de Ecuador con los estándares internacionales es la falta de reconocimiento de ciertos preceptos normativo expreso, como la privacidad desde el diseño (privacy by design) y la privacidad por defecto (privacy by default), ampliamente adoptados por el Reglamento General de Protección de Datos de la Unión Europea y respaldados por organismos internacionales como el Consejo de Europa y la Organización para la Cooperación y el Desarrollo Económicos. Estos principios exigen a los responsables del tratamiento adoptar medidas proactivas desde las fases iniciales de diseño de cualquier sistema que procese datos personales, con el fin de garantizar que la privacidad esté incorporada de forma estructural y no como un complemento posterior (Sánchez Esparza, 2023).

También debe considerarse que el Ecuador ha avanzado recientemente en el establecimiento de mecanismos para la transferencia internacional de datos, aspecto central en la gobernanza global de la privacidad. El Reglamento General de Protección de Datos regula con precisión las condiciones bajo las cuales puede transferirse información personal fuera del Espacio Económico Europeo, exigiendo garantías

adecuadas mediante decisiones de adecuación, cláusulas contractuales tipo o normas corporativas vinculantes. En el caso ecuatoriano, la Ley Orgánica de Protección de Datos Personales incorpora un marco regulatorio específico en sus capítulos V y IX, reforzado por la Resolución SPDP-SPD-2025-0024-R de la Superintendencia de Protección de Datos Personales, que desarrolla los procedimientos y garantías aplicables a las transferencias nacionales e internacionales. No obstante, a pesar de estos avances normativos, persisten desafíos en cuanto a la implementación práctica, la supervisión constante del nivel de protección en países terceros y la consolidación de criterios uniformes que aseguren una interoperabilidad plena con marcos jurídicos más desarrollados (Superintendencia de Protección de Datos Personales, 2025; Asamblea Nacional, 2021; Parlamento Europeo y Consejo de la Unión Europea, 2016)

También debe considerarse el limitado avance del Ecuador en el establecimiento de mecanismos eficaces para la transferencia internacional de datos, aspecto central en la gobernanza global de la privacidad. El Reglamento General de Protección de Datos de la Unión Europea regula con precisión las condiciones bajo las cuales puede transferirse información personal fuera del Espacio Económico Europeo, exigiendo garantías adecuadas mediante decisiones de adecuación, cláusulas contractuales tipo o normas corporativas vinculantes. La Ley Orgánica de Protección de Datos Personales de Ecuador, junto con sus reglamentos y las resoluciones de la Superintendencia, regula la transferencia internacional de datos personales, estableciendo que el país u organización receptora debe contar con un nivel de protección adecuado o, en su defecto, que se apliquen garantías apropiadas como cláusulas contractuales tipo, normas corporativas vinculantes o mecanismos similares. Sin embargo, dentro de este marco regulatorio, cabe señalar que existen problemas, tanto en el aspecto técnico como en la falta de estandarización, que dificultan el uso de criterios para determinar el "nivel de protección equivalente" en otros países. Esto, a su

vez, genera un riesgo limitante en cuanto a la interoperabilidad del sistema ecuatoriano y su plena compatibilidad con sistemas jurídicos más avanzados, como por ejemplo, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

La normativa técnica exige una visión integral de los derechos humanos que impida que la protección de datos personales se convierta en una mera cuestión procedimental, y que la entienda como un asunto sustantivo para la salvaguarda de la dignidad humana. En el ámbito del Derecho Laboral, esto implica el deber de evitar que las tecnologías de control, incluidos los sistemas de identificación biométrica, se conviertan en instrumentos de vigilancia excesiva, discriminación indirecta o violación de derechos fundamentales. A diferencia de lo que establece la guía del Reglamento General de Protección de Datos (RGPD) y el enfoque holístico de los organismos internacionales en la salvaguarda de los derechos fundamentales, en Ecuador la normativa vigente no establece de forma explícita esta interrelación y, por lo tanto, dificulta la adopción de un enfoque matricial integrador basado en garantías, especialmente en contratos laborales asimétricos (Aida Martínez García, 2025).

En el ámbito laboral, donde el tratamiento de datos biométricos plantea riesgos elevados para la privacidad y los derechos fundamentales, esta falta de alineación con el estándar europeo y con las directrices internacionales como las emitidas por la Organización para la Cooperación y el Desarrollo Económicos, el Consejo de Europa y la Comisión Interamericana de Derechos Humanos resulta particularmente preocupante.

CAPITULO III

Desarrollo Jurisprudencial en Ecuador Sobre la Protección de Datos Personales

3.1. Análisis de sentencias relevantes de la Corte Constitucional del Ecuador

3.1.1. Análisis de Sentencia No. 2064-14-EP/21

La Sentencia No. 2064-14-EP/21, emitida por el Pleno de la Corte Constitucional del Ecuador el 27 de enero de 2021, constituye un punto de inflexión en la jurisprudencia constitucional ecuatoriana sobre la protección de datos personales, al transitar desde una visión procesal del hábeas data hacia una comprensión sustantiva de los derechos que lo sustentan. Esta resolución no solo reconoce la protección de datos como un derecho independiente, sino que también indica que su vulneración puede producirse en el momento en que se procesan datos sin fundamento jurídico ni consentimiento válido, sin necesidad de demostrar un daño posterior. Al hacerlo, la Corte redefine el alcance del principio de legalidad, posicionándolo como el eje central en lo relativo al tratamiento de la información personal, incluso en casos complejos como el ámbito laboral, donde el uso de datos biométricos se ha vuelto una práctica cada vez más común. (Corte Constitucional del Ecuador, 2021).

El caso relativo a la posesión y el tratamiento no autorizado de fotografías íntimas permitió a la Corte formular criterios interpretativos que tienen un impacto directo en el tratamiento de datos considerados de alto riesgo, en particular los datos biométricos. La Corte consideró que la obtención o la retención de datos personales sin consentimiento previo, libre y expreso, constituye una violación del derecho a la autodeterminación informativa (Corte Constitucional del Ecuador, 2021). Este criterio, en el ámbito laboral, revela que el empleador no puede justificar el tratamiento de datos biométricos de sus empleados únicamente con base en la subordinación contractual. La asimetría existente entre empleador y empleado crea un contexto en el que el consentimiento, en sentido estricto, no es libre, lo cual constituye una violación del principio de legalidad, ya que la información se obtuvo sin

una base jurídica específica establecida en la Ley Orgánica de Protección de Datos Personales.

Además, la Corte propone una interpretación importante del concepto de “tratamiento de datos personales” al extender su alcance a la recopilación, circulación, almacenamiento, archivo o mera posesión de información sin justificación legal (Corte Constitucional del Ecuador, 2021). Esta interpretación se ajusta a lo dispuesto en la Constitución, específicamente en el artículo 66, numeral 19, que afirma el derecho a controlar la información personal y a defenderla contra el tratamiento ilícito. En el contexto del derecho laboral, esto implica que la sola instalación de dispositivos de control biométrico sin una justificación legal y sin superar el test de proporcionalidad puede configurar una violación constitucional, incluso antes de que exista un daño material. De esta forma, la Corte consolida una lectura preventiva del derecho a la protección de datos, en la cual el principio de legalidad actúa como una barrera inicial frente al uso arbitrario de tecnologías de identificación.

Otro aspecto de especial trascendencia en la sentencia es la delimitación del ámbito doméstico frente al interés constitucional en la tutela de los datos personales. La Corte sostiene que el carácter privado de la información o de los medios donde se almacena no excluye la intervención constitucional cuando la información compromete derechos fundamentales (Corte Constitucional del Ecuador, 2021). Esta idea tiene una proyección directa en el ámbito empresarial, en el que el manejo de datos biométricos se realiza en entornos internos, pero puede implicar riesgos sustanciales para los trabajadores. Por lo tanto, el control biométrico de asistencia o el control de acceso a las instalaciones también está sujeto a control legal, ya que la razón interna para el uso de los datos no significa que se puedan pasar por alto los principios de proporcionalidad, necesidad y finalidad legítima, que exige la Ley Orgánica de Protección de Datos.

Desde una perspectiva crítica, esta sentencia logró desplazar el análisis del tratamiento de datos de un enfoque formalista a uno sustantivo y protector. El Tribunal señala que el consentimiento, cuando se obtiene en situaciones de dependencia y subordinación, como en el caso de las relaciones laborales, puede estar viciado y, por consiguiente, no puede ser la única fuente de legitimación del tratamiento. Este enfoque confronta la práctica empresarial que justifica la recopilación de datos biométricos únicamente con base en el consentimiento contractual, alegando que los trabajadores tienen libertad de decisión, cuando en realidad el consentimiento implica condiciones de elección y ausencia de presión por parte de la jerarquía.

En este contexto, el principio de legalidad exige que todo tratamiento se base en una norma que lo autorice y que además supere los criterios de proporcionalidad a que se refieren los artículos 10 y 26 de la Ley Orgánica de Protección de Datos, de tal manera que la medida sea adecuada, necesaria y no desproporcionada en relación con el fin perseguido.

En consecuencia, la sentencia 2064-14-EP/21 refuerza la obligación de los responsables del tratamiento de datos personales, incluidos los empleadores públicos y privados, de realizar evaluaciones de impacto, análisis de riesgos y pruebas de proporcionalidad antes de implementar cualquier forma de vigilancia biométrica (Corte Constitucional del Ecuador, 2021). Estas responsabilidades van más allá de meras formalidades técnicas; constituyen, de hecho, medios concretos para la realización de un principio jurídico, cuya legalidad exige la justificación tanto de derecho como de hecho de cualquier tratamiento en cuestión. Al ordenar la eliminación definitiva de las imágenes y la prohibición de su uso futuro, el Tribunal demuestra que un remedio constitucional debe estar dirigido a prevenir la repetición del tratamiento ilícito, en lugar de limitarse a paliar el impacto del tratamiento previo. En el ámbito laboral, esto requiere, en principio, la implementación de medidas técnicas y organizativas para garantizar que los datos biométricos se eliminen de

forma irreversible al finalizar la relación laboral, suprimiendo así el riesgo continuo de uso ilícito de dichos datos.

La relevancia de este fallo en el marco de la Ley Orgánica de Protección de Datos Personales se manifiesta en su reafirmación de que el principio de legalidad es la primera garantía frente a cualquier forma de tratamiento automatizado. El reconocimiento de la ilicitud por la sola ausencia de base jurídica o consentimiento válido constituye una evolución jurisprudencial que fortalece la tutela de los datos biométricos frente a su uso arbitrario en entornos laborales.

3.1.2. Análisis de Sentencia No. 182-15-SEP-CC

La Sentencia No. 182-15-SEP-CC, emitida por el Pleno de la Corte Constitucional del Ecuador el 15 de julio de 2015, resolvió una acción extraordinaria de protección planteada por una ciudadana contra una resolución del Consejo de la Judicatura que había dispuesto la desvinculación de varios servidores judiciales como parte de un proceso de evaluación y reestructuración institucional. La accionante alegó que dicha desvinculación vulneró sus derechos constitucionales al trabajo, a la estabilidad laboral, al debido proceso, a la seguridad jurídica y, especialmente, al derecho a la protección de sus datos personales, ya que la evaluación que dio lugar a su desvinculación se basó en un sistema automatizado que procesaba información personal y profesional sin que existiera transparencia, consentimiento o posibilidad real de impugnación. En este contexto, la Corte Constitucional centró su análisis en el tratamiento de los datos utilizados por el Consejo de la Judicatura para justificar decisiones que afectaban directamente la vida laboral de los evaluados (Corte Constitucional del Ecuador, 2015).

El fallo es relevante porque la Corte reconoce que los sistemas de evaluación que recopilan, almacenan, procesan y valoran datos personales, aunque tengan fines institucionales legítimos están sujetos a los límites constitucionales del derecho a la protección de datos, a la

autodeterminación informativa y al principio de legalidad. La Corte determinó que el Consejo de la Judicatura utilizó criterios y herramientas de calificación que implicaban un tratamiento automatizado de datos, sin garantizar el acceso de los evaluados a la información que se procesaba, ni permitirles conocer la lógica, metodología o ponderación de los indicadores que definían su permanencia o salida del cargo (Corte Constitucional del Ecuador, 2015). Esta opacidad fue considerada una forma de vulneración del derecho a la protección de datos, ya que el tratamiento fue realizado sin consentimiento informado, sin base legal clara, y sin mecanismos efectivos para ejercer los derechos de acceso, rectificación o impugnación.

En este sentido, la Corte Constitucional afirmó que el tratamiento de datos personales no se limita al almacenamiento o archivo de información, sino que abarca toda forma de uso, análisis, evaluación o interconexión de datos que pueda tener efectos jurídicos sobre la persona titular (Corte Constitucional del Ecuador, 2015). En este caso, la evaluación automatizada realizada por el Consejo de la Judicatura produjo consecuencias concretas sobre la situación laboral de la accionante, y por tanto requería cumplir con los principios constitucionales de legalidad, finalidad, proporcionalidad, transparencia y control ciudadano. El hecho de que el sistema fuera implementado por una entidad pública no exime de responsabilidad ni elimina la necesidad de garantizar la autodeterminación informativa de los funcionarios evaluados.

El razonamiento de la Corte en esta sentencia se conecta directamente con los postulados de la Ley Orgánica de Protección de Datos Personales que, aunque fue promulgada años después, reconoce como principios rectores del tratamiento de datos: la licitud, la finalidad específica, la minimización de datos, la transparencia y la responsabilidad proactiva del responsable del tratamiento. La Corte, de manera anticipada, ya advertía que los procesos institucionales que impliquen recopilación y análisis de datos personales deben tener una base jurídica

clara y deben respetar los derechos de los titulares sobre su propia información. En el caso analizado, no se informó de manera adecuada a los evaluados sobre el uso de sus datos ni se les permitió ejercer control sobre los mismos, lo cual configuró una violación constitucional (Corte Constitucional del Ecuador, 2015).

Desde el punto de vista central el tratamiento de datos personales en el ámbito laboral, especialmente los datos biométricos esta sentencia aporta criterios esenciales. Primero, establece que cuando una institución trata datos de sus trabajadores con el fin de evaluar su desempeño, eficiencia o permanencia, ese tratamiento debe respetar los derechos fundamentales del trabajador. Segundo, señala que el uso de herramientas automatizadas, algoritmos o sistemas informáticos para tomar decisiones laborales no puede estar exento de transparencia ni de control por parte del titular de los datos. Tercero, refuerza la idea de que la relación laboral no implica una renuncia automática a los derechos sobre los propios datos, ni permite que el empleador sea público o privado disponga libremente de la información personal del trabajador sin su consentimiento y sin su participación activa en el proceso.

La Corte también enfatiza que la protección de datos personales se extiende al entorno laboral porque el poder disciplinario o administrativo de la institución no es ilimitado (Corte Constitucional del Ecuador, 2015). La estabilidad laboral, la honra, la dignidad y el derecho a no ser objeto de decisiones arbitrarias basadas en información que el trabajador no conoce ni puede impugnar forman parte del núcleo de la autodeterminación informativa. Así, el tratamiento de datos en el contexto de relaciones laborales debe estar sometido a control judicial cuando existe una afectación concreta de derechos. Este principio puede ser extrapolado al tratamiento de datos biométricos, que son aún más sensibles por su carácter único, permanente e irremplazable. En consecuencia, cualquier sistema de control laboral que utilice datos biométricos debe contar con una base legal expresa, con consentimiento libre e informado, y con

garantías de seguridad, confidencialidad y limitación temporal del tratamiento.

Esta sentencia constituye un antecedente importante en la construcción de un bloque jurisprudencial que articula el derecho a la protección de datos personales con otros derechos laborales fundamentales. Al sancionar la opacidad y la falta de participación en los procesos de evaluación basados en datos personales, la Corte sienta un precedente que protege a los trabajadores frente a decisiones automatizadas o arbitrarias que puedan afectar su vida profesional. De esta manera, se configura una doctrina que considera al titular de los datos no como un sujeto pasivo, sino como un actor con derecho a intervenir, conocer, corregir y oponerse al tratamiento de su información, especialmente cuando dicho tratamiento puede determinar su continuidad en el empleo.

3.1.3. Análisis de Sentencia No. 1068-19-JP/25

La Sentencia No. 1068-19-JP/25, emitida por la Corte Constitucional del Ecuador en febrero de 2025, constituye un hito en la consolidación del derecho a la protección de datos personales como un componente esencial del principio de legalidad y de la dignidad humana. Esta sentencia se centró en las telecomunicaciones, pero sus consecuencias jurídicas son importantes para todos los ámbitos que impliquen el tratamiento de datos personales, incluido el laboral. El caso se originó a raíz de una acción de amparo interpuesta por la Defensoría del Pueblo en nombre de sesenta y cinco personas contra OTECEL SA (Movistar) por cobro abusivo de datos, imputación de deudas y gestión de cobros. Movistar también trató y compartió datos personales sin consentimiento válido ni fundamento jurídico. Este caso permitió a la Corte perfeccionar sus criterios estructurales sobre la licitud del tratamiento de datos, la responsabilidad de los responsables del tratamiento y los derechos y obligaciones de los encargados del

tratamiento para garantizar la integridad, la confidencialidad y la legitimidad de los datos durante todo el proceso (Corte Constitucional del Ecuador, 2025).

El marco central de la sentencia se basa en el principio de que una empresa privada que presta el servicio de telefonía móvil «realiza una actividad pública» y, por lo tanto, tiene las mismas obligaciones de responsabilidad y protección que cualquier entidad estatal, dado que dicha actividad también implica el tratamiento de un número significativo de datos personales sensibles. La Corte Constitucional del Ecuador (2025) argumentó, asimismo, que OTECEL vulneró el derecho constitucional a la protección de datos (art. 66, núm. 19) al no verificar la identidad de los contratistas ni las obligaciones económicas y contractuales vinculantes para las partes, las cuales se crearon con base en datos no consentidos ni validados. Este argumento se deriva del principio de legalidad, que establece que todo tratamiento de datos debe tener una base jurídica o contar con el consentimiento del titular de los datos, el cual debe ser libre, específico e informado. La ausencia de cualquiera de estas condiciones convierte el tratamiento en ilícito y constituye una violación de un derecho personal.

La perspectiva crítica adoptada sobre esta frase reafirma el argumento de que la legitimidad del tratamiento legal de datos personales no puede defenderse únicamente en función del propósito económico o administrativo del titular, sino en la aplicación ética de los principios legales de necesidad, proporcionalidad y transparencia. En 2025, la Corte Constitucional del Ecuador dictaminó que la negligencia de OTECEL al no proporcionar mecanismos adecuados para la identificación de una persona constituía una negligencia que derivó en el tratamiento masivo de datos peligrosos y sin control. Este razonamiento es aplicable al ámbito laboral en lo que respecta al uso de datos biométricos, donde el control de la identidad y la gestión de datos sensibles implican el control sobre los datos personales del individuo. En ambos casos, el riesgo de un tratamiento abusivo de los datos se agrava cuando las instituciones no

realizan una evaluación de impacto sobre la privacidad de los datos y carecen de consentimiento informado. Esto ilustra un escenario en el que la tecnología, al carecer de justificación legal y mecanismos de control adecuados, se convierte en una herramienta para la violación de derechos.

Además, la Corte establece un estándar vinculante sobre el principio de licitud del tratamiento de datos personales: todo tratamiento debe tener una base legal, verificable y adecuada a los fines declarados. En el caso de OTECEL, el uso no autorizado de la identidad, las cuentas bancarias y demás información de una persona constituyó un tratamiento de datos contrario a sus derechos. La Corte extendió esta lógica a la obligación del Estado, ordenando a ARCOTEL y a la Superintendencia de Protección de Datos Personales que emitieran una norma específica sobre los procedimientos de verificación de identidad y la regulación de datos de los usuarios (Corte Constitucional del Ecuador, 2025). Esta directiva, si bien se enmarca en el contexto de la contratación de servicios, es plenamente aplicable al ámbito laboral, donde el empleador también actúa como responsable del tratamiento de los datos y debe garantizar que el procesamiento de datos biométricos se realice de manera lícita, proporcional y con un fin específico.

Una de las dimensiones que la jurisprudencia debe aportar es la conceptualización, por parte de la Corte, de la responsabilidad reforzada del responsable del tratamiento de datos. Se ha señalado que incluso la negligencia que no causa daño y que no pone a prueba la implementación de medidas técnicas y organizativas constituye una violación constitucional (Corte Constitucional del Ecuador, 2025). Esta tendencia se alinea con la obligación establecida en los artículos 40 y 41 de la Ley Orgánica de Protección de Datos Personales, que estipula que, antes de cualquier tratamiento, deben identificarse los riesgos, las amenazas y las vulnerabilidades. En consecuencia, la Corte sostiene que se requiere responsabilidad proactiva y debida diligencia para demostrar el principio de legalidad, con documentación, registros y evaluaciones verificables.

Desde un punto de vista sustantivo, la sentencia pretende reafirmar la relación entre el derecho al tratamiento de datos personales y la dignidad humana, señalando que el uso de datos sin autorización o de manera indebida afecta a la parte íntima de la persona, en lo que respecta a su honor, su reputación y su proyecto de vida.. Este enfoque encuentra correlato con la doctrina internacional, especialmente con el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 11 de la Convención Americana sobre Derechos Humanos, que prohíben injerencias arbitrarias en la vida privada. De este modo, la Corte ecuatoriana consolida un bloque de constitucionalidad informacional que trasciende el caso concreto, situando al titular de los datos como el centro del sistema jurídico de protección.

3.2. Análisis de Jurisprudencia administrativa de la Superintendencia de Protección de Datos Personales

3.2.1. Oficio N° SPDP-IRD-2025-0031-O de marzo de 2025

La Ley Orgánica de Protección de Datos Personales (LOPDP) y su reglamento desarrollan el contenido sustantivo de este derecho, determinando que el tratamiento de datos personales solo puede realizarse con base en principios como la licitud, la finalidad, la proporcionalidad, la minimización, la seguridad y la confidencialidad (Asamblea Nacional, 2021). Esto implica que el responsable del tratamiento tiene una obligación positiva de adoptar medidas técnicas y organizativas adecuadas que garanticen la confidencialidad, disponibilidad e integridad de los datos durante todo su ciclo de vida.

La Ley Orgánica de Protección de Datos Personales distingue dos grandes categorías de datos personales: los datos generales y los datos especiales. Dentro de los datos especiales se encuentran los datos personales sensibles, que incluyen los datos biométricos, entendidos como información única e intransferible relacionada con características físicas, fisiológicas o conductuales de la persona, tales como huellas

dactilares, patrones faciales, iris, voz o ADN. Esta categoría, al pertenecer a la esfera más íntima del individuo, merece una protección reforzada, motivo por el cual la ley establece una prohibición general de tratamiento, salvo que concurra alguna de las excepciones taxativamente previstas en el artículo 26 de la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021). Estas excepciones incluyen, entre otras, el consentimiento del titular, el cumplimiento de obligaciones o ejercicio de derechos en el ámbito laboral, la protección de intereses vitales, la publicación manifiesta de los datos por el titular, mandato judicial o el tratamiento con fines de investigación o archivo en interés público.

Sin embargo, al analizar estas excepciones en relación con el uso de datos biométricos para el registro de asistencia laboral, se evidencia que ninguna de ellas resulta aplicable de manera legítima. En primer lugar, la excepción relativa al cumplimiento de obligaciones laborales no es pertinente, dado que en la normativa ecuatoriana no existe disposición alguna que obligue a los empleadores, sean personas naturales o jurídicas, a utilizar sistemas biométricos como método de control de asistencia. El artículo 26 literal b de la Ley Orgánica de Protección de Datos Personales no puede interpretarse extensivamente para justificar un tratamiento que invade la esfera más íntima del trabajador, cuando existen medios alternativos menos intrusivos y plenamente eficaces para cumplir con la misma finalidad (Corte Constitucional del Ecuador, 2021). En segundo lugar, las excepciones relativas a la protección de intereses vitales o a la publicación manifiesta de datos no se configuran, pues los empleados son plenamente capaces y no han hecho públicos sus rasgos biométricos en ningún medio. De igual manera, la hipótesis de orden judicial carece de fundamento, ya que una disposición de esa naturaleza sería inconstitucional por vulnerar los derechos a la privacidad y a la autodeterminación informativa.

En el ámbito del consentimiento, el análisis requiere mayor profundidad, pues esta base legitimadora se encuentra en el núcleo del

debate sobre la validez del tratamiento biométrico en relaciones de subordinación laboral. La Ley Orgánica de Protección de Datos Personales define que el consentimiento debe ser libre, específico, informado e inequívoco. No obstante, la característica de “libre” se ve comprometida en contextos donde existe una relación de poder o dependencia. De acuerdo con el artículo 1472 del Código Civil ecuatoriano, el consentimiento se encuentra viciado por fuerza cuando media un temor grave o irreparable, y si bien el “temor reverencial” entendido como el simple miedo a desagradar a una autoridad o superior no basta para anular el consentimiento, la doctrina advierte que este concepto debe analizarse con base en el equilibrio real entre las partes (Asamblea Nacional, 2005, art. 1472). En el entorno laboral, la subordinación económica y jerárquica genera un desequilibrio estructural que impide considerar libre la voluntad del trabajador frente a su empleador. El trabajador depende de su salario para subsistir y teme perder su fuente de ingresos si no acepta las condiciones impuestas, lo que transforma el temor reverencial en un temor real y coactivo que vicia el consentimiento desde el punto de vista jurídico (Corte Interamericana de Derechos Humanos, 2018).

Esta interpretación es congruente con los estándares internacionales en materia de derechos humanos. La Corte Interamericana de Derechos Humanos ha sostenido que el consentimiento no puede considerarse libre cuando la negativa a otorgarlo podría implicar la pérdida del empleo o la restricción de derechos fundamentales, pues en esos casos la relación de poder transforma la manifestación de voluntad en un acto condicionado por necesidad (Corte Interamericana de Derechos Humanos, 2018). En consecuencia, exigir el consentimiento del trabajador para registrar su asistencia mediante sistemas biométricos constituye una forma indirecta de coacción incompatible con los principios de dignidad humana, libertad de trabajo y vida digna consagrados en los artículos 33 y 66 numeral 2 de la CRE (Constitución de la República del Ecuador, 2008).

Además, la aplicación de los principios de pertinencia, minimización y proporcionalidad refuerza la invalidez del uso de datos biométricos en estos casos. Según la Ley Orgánica de Protección de Datos Personales (art. 8), los datos personales tratados deben ser adecuados, pertinentes y limitados a lo estrictamente necesario para cumplir con la finalidad legítima prevista. El principio de proporcionalidad exige que el tratamiento no sea excesivo en relación con el propósito perseguido. En este contexto, la finalidad de registrar la asistencia de los trabajadores puede cumplirse mediante mecanismos menos invasivos como tarjetas magnéticas, contraseñas, registros manuales o validaciones digitales no biométricas, que no afectan la intimidad del titular ni implican el tratamiento de datos sensibles. Por tanto, el uso de sistemas biométricos carece de proporcionalidad, pues vulnera el principio de minimización al recolectar información que excede lo necesario para la finalidad propuesta (Asamblea Nacional, 2021).

Por otro lado, la gestión del riesgo en el tratamiento de datos biométricos adquiere relevancia especial. La Ley Orgánica de Protección de Datos Personales dispone que cuando un tratamiento represente un riesgo alto para los derechos de los titulares, el responsable debe realizar una evaluación de impacto previa (Asamblea Nacional, 2021, art. 37). Los datos biométricos, por su naturaleza única e irreversible, implican un riesgo particularmente elevado, ya que una filtración, pérdida o uso indebido de la información no puede ser revertido ni sustituido, a diferencia de otros datos personales. La omisión de esta evaluación preventiva no solo implica incumplimiento normativo, sino también responsabilidad administrativa e incluso civil por parte del responsable del tratamiento. De acuerdo con la jurisprudencia reciente de la Superintendencia de Protección de Datos Personales (Superintendencia de Protección de Datos Personales, 2025), el uso de biometría laboral sin justificación ni evaluación de riesgos constituye una práctica desproporcionada e ilegítima, contraria a los principios constitucionales de legalidad y finalidad.

3.2.2. Oficio N° SPDP-IRD-2025-0108-O de agosto de 2025

El análisis realizado por la Superintendencia de Protección de Datos Personales parte de una base constitucional sólida, sustentada en los artículos 33, 66 numerales 2, 17 y 19, y 92 de la Constitución de la República del Ecuador (CRE)**,** que garantizan el derecho al trabajo digno, a la libertad de trabajo y al derecho a la protección de datos personales. La autoridad reconoce que la dignidad humana y la autodeterminación informativa constituyen pilares de todo tratamiento de datos personales, y que la relación laboral por su naturaleza jerárquica y dependiente debe ser analizada con especial precaución cuando involucra información biométrica del trabajador. Por ello, la Superintendencia de Protección de Datos Personales establece que el consentimiento en estos casos no puede considerarse libre si el titular no tiene la posibilidad real de elegir entre distintas alternativas no invasivas para el control de asistencia, pues la subordinación económica y jerárquica genera un riesgo de coacción implícita (Asamblea Nacional Constituyente, 2008).

El pronunciamiento reitera la prohibición general del tratamiento de datos personales sensibles, dispuesta en el artículo 26 de la Ley Orgánica de Protección de Datos Personales (LOPDP), salvo que concurra una de las excepciones expresamente reconocidas por la ley. Entre ellas se encuentra el consentimiento explícito del titular, siempre que cumpla con los requisitos de ser libre, específico, informado e inequívoco (Asamblea Nacional, 2021). No obstante, la Superintendencia de Protección de Datos Personales deja claro que el consentimiento no puede entenderse como una base legitimadora automática: este debe ser precedido por el cumplimiento de tres requisitos ineludibles el test de proporcionalidad**,** el análisis de riesgo y la evaluación de impacto. Solo si estos procedimientos determinan que el tratamiento no genera un riesgo alto o crítico para los derechos del titular, el consentimiento podrá ser considerado jurídicamente válido (Superintendencia de Protección de Datos Personales, 2025).

El test de proporcionalidad, de acuerdo con lo dispuesto en el artículo 10 literal f de la Ley Orgánica de Protección de Datos Personales, busca determinar si el tratamiento de datos es adecuado, necesario y no excesivo en relación con la finalidad perseguida. En este sentido, la Superintendencia de Protección de Datos Personales sostiene que el registro de asistencia laboral puede cumplirse mediante mecanismos menos invasivos como tarjetas electrónicas, contraseñas personales o registros digitales de ingreso, que no impliquen la captura y almacenamiento de información biométrica. Por tanto, la recolección de datos dactiloscópicos o faciales para este fin resulta desproporcionada si no se demuestra que otras alternativas no pueden garantizar la misma eficacia.

En lo que respecta al análisis de riesgos y la evaluación de impacto, la Superintendencia de Protección de Datos Personales subraya la necesidad de que el responsable del tratamiento reconozca los riesgos y vulnerabilidades que puedan derivarse de la implementación de la tecnología biométrica. De conformidad con los artículos 40, 41 y 42 de la Ley Orgánica de Protección de Datos Personales, dicha evaluación debe tener en cuenta la naturaleza de los datos, el contexto del tratamiento, las partes interesadas y los antecedentes relacionados con incidentes de seguridad. La finalidad de estos procedimientos es prevenir filtraciones, accesos no autorizados y daños irreversibles al derecho a la privacidad del titular. En caso de detectarse riesgos altos o críticos, el tratamiento debe ser suspendido o rediseñado hasta que se implementen medidas de mitigación adecuadas (Asamblea Nacional, 2021).

Uno de los aportes doctrinales más relevantes del oficio radica en su interpretación del consentimiento libre en contextos laborales, en concordancia con el artículo 1472 del Código Civil, que regula los vicios del consentimiento. La Superintendencia de Protección de Datos Personales reconoce que en la relación empleador trabajador existe un desequilibrio de poder que puede convertir el temor reverencial entendido

como el simple miedo a desagradar al superior en un temor real de perder el empleo, lo cual constituye una forma de coacción incompatible con el principio de libertad. Por tanto, el consentimiento otorgado en estas condiciones se considera jurídicamente inválido, puesto que se encuentra viciado por la falta de autonomía real del titular (Asamblea Nacional, 2005,).

La autoridad administrativa complementa este análisis con una interpretación coherente de los principios rectores del tratamiento de datos personales, especialmente los de pertinencia, minimización y proporcionalidad, consagrados en el artículo 10 de la Ley Orgánica de Protección de Datos Personales. En su criterio, el responsable debe recolectar únicamente los datos estrictamente necesarios para cumplir con una finalidad específica, y el uso de tecnologías biométricas no puede justificarse cuando existen medios alternativos menos intrusivos. Este razonamiento refleja la aplicación práctica del principio de necesidad, desarrollado por el Tribunal de Justicia de la Unión Europea en materia de protección de datos, y demuestra la convergencia del ordenamiento ecuatoriano con los estándares internacionales de protección reforzada de los datos sensibles (Corte de Justicia de la Unión Europea, 2018).

Por otra parte, el pronunciamiento aborda la aplicabilidad del derecho de acceso y del derecho de rectificación, previstos en los artículos 13 y 14 de la Ley Orgánica de Protección de Datos Personales. La Superintendencia de Protección de Datos Personales reitera los requisitos del principio de transparencia en relación con los trabajadores y exempleados. Tienen derecho a solicitar copias de todos los contratos, nóminas y documentos de ingreso y salida del IESS que contengan sus datos personales, independientemente del motivo de la solicitud. Esta disposición busca el equilibrio entre el control de los datos personales y la responsabilidad del responsable del tratamiento. Respecto al derecho de rectificación, la Superintendencia de Protección de Datos Personales indica que este solo se aplicará si el interesado aporta la documentación

probatoria requerida o una resolución judicial firme que declare la inexactitud de los datos. Esta disposición tiene como objetivo proteger la seguridad jurídica y al interesado frente al posible abuso de este derecho (2025).

La Superintendencia de Protección de Datos Personales, en su parte final, establece que el interés general no puede ni debe considerarse una base legitimadora autónoma para el tratamiento de datos personales, ya que no se reconoce como tal en la Constitución de la República ni en la Ley Orgánica de Protección de Datos Personales. La declaración en cuestión, de carácter no especulativo, reviste suma importancia, pues impedirá que entidades público-privadas aleguen el abuso del argumento de la eficiencia administrativa, que ignora la posibilidad de procedimientos negligentes que pueden vulnerar gravemente la privacidad y la autodeterminación informativa de una persona. De este modo, la autoridad establece los parámetros de lo que puede y no puede legitimarse en el uso de la información personal, haciendo hincapié en la legalidad, que es y seguirá siendo uno de los principios fundamentales para dicho uso.

3.3. Eficacia jurisprudencial respecto al tratamiento de datos biométricos en el Ecuador

Ecuador, en materia de protección de datos y relaciones laborales contemporáneas, ha comenzado a construir un marco interpretativo armonioso que, si bien aún se encuentra en consolidación, ha empezado a sentar las bases para el desarrollo de argumentos en su implementación. Es precisamente en la aplicación de este marco donde persisten las tensiones entre las disposiciones constitucionales, la informalidad en la gestión de datos y las tecnologías disponibles. Junto a los pronunciamientos administrativos de la Superintendencia de Protección de Datos Personales (SPDP), las decisiones de la Corte Constitucional conforman un corpus interpretativo que, por un lado, ilustra

una mayor protección operativa del derecho al consentimiento y de los principios de proporcionalidad jurídica en el tratamiento de datos sensibles, y por otro, expone los persistentes desafíos de la ineficiencia material y la disonancia institucional (Corte Constitucional del Ecuador, 2021).

En cuanto a la jurisprudencia, la Corte Constitucional ha declarado que el derecho a la autodeterminación informativa abarca la protección de datos personales y, por lo tanto, constituye una limitación al control (público o privado) sobre la información de una persona. En la Sentencia N.° 182-15-SEP-CC (2015), la Corte afirmó que la información personal debe tratarse conforme a los principios de licitud, finalidad, proporcionalidad y necesidad, y que la falta de consentimiento o el consentimiento obtenido mediante subordinación o coacción constituye una violación directa del derecho fundamental a la privacidad y la dignidad de la persona (Corte Constitucional del Ecuador, 2015). Esto reviste gran importancia en el ámbito laboral, ya que la relación de trabajo se caracteriza por la presunción de parcialidad contra el empleado. En este caso, no puede presumirse libremente el consentimiento del empleado para el tratamiento de sus datos biométricos.

Ilustro el razonamiento de la reciente Sentencia N.° 1068-19-JP/25 (2025) en el sentido de que la recopilación de información biométrica debe superar la prueba de proporcionalidad en sentido estricto, considerando que debe ser apropiada, necesaria y estrictamente proporcional al objetivo perseguido. La Corte sostiene específicamente que los datos biométricos en los contratos de trabajo y el control de asistencia laboral son una condición obligatoria y que, en ausencia de consentimiento para el tratamiento de dichos datos, debe realizarse un análisis de riesgos y una evaluación de los impactos sobre los derechos del trabajador. El consentimiento, por sí solo, no debe legitimar el tratamiento si no se demuestran medios menos invasivos, ya que, debido a la naturaleza de los datos, se requiere otro tratamiento (Corte

Constitucional del Ecuador, 2025). Evidentemente, esto se traduce en un cambio en la concepción del consentimiento, que ahora se estudia desde una perspectiva sustantiva, en contraste con la mera formalidad del contrato.

Las comunicaciones administrativas de la Superintendencia de Protección de Datos Personales, en particular las núms. SPDP-IRD-2025-0031-O y SPDP-IRD-2025-0072-O, consolidan una línea interpretativa restrictiva respecto al uso de datos biométricos como principal herramienta de control laboral. Dichas comunicaciones indican que el uso de la biometría como tal solo se admite como último recurso, una vez agotadas las opciones menos invasivas y tras superar satisfactoriamente las pruebas de proporcionalidad, evaluación de riesgos y evaluación de impacto (Superintendencia de Protección de Datos Personales, 2025).Esta interpretación amplía el margen de protección de los trabajadores, al reconocer que la subordinación laboral impide presumir la libertad del consentimiento, incluso cuando el trabajador aparentemente acepta el tratamiento de sus datos.

Sin embargo, la eficacia de esta jurisprudencia y de los pronunciamientos administrativos enfrenta desafíos importantes. En la práctica, muchas instituciones públicas y privadas continúan implementando sistemas biométricos sin cumplir con los estándares de evaluación de impacto o sin demostrar la proporcionalidad del tratamiento, lo cual evidencia una brecha entre la norma jurídica y su efectividad real. Esta situación plantea la necesidad de fortalecer los mecanismos de supervisión y sanción de la Superintendencia de Protección de Datos Personales, así como de dotar a los jueces de mayores herramientas técnicas para evaluar la proporcionalidad del tratamiento de datos en contextos laborales (Superintendencia de Protección de Datos Personales, 2025).

En términos críticos, si bien las sentencias y oficios constituyen avances interpretativos relevantes, su eficacia depende de la capacidad institucional para garantizar la aplicación efectiva de los principios de minimización y necesidad. El test de proporcionalidad, tal como lo ha estructurado la Corte Constitucional, se presenta más como una guía hermenéutica que como un instrumento operativo, lo que limita su alcance práctico frente a las dinámicas empresariales contemporáneas. De este modo, la eficacia jurisprudencial se encuentra condicionada por la débil cultura de cumplimiento en materia de protección de datos y por la ausencia de una doctrina judicial consolidada que permita uniformar los criterios interpretativos entre la Corte Constitucional y la autoridad administrativa.

Discusión

El análisis efectuado evidencia que la protección de datos personales biométricos en el Ecuador, si bien ha alcanzado avances normativos significativos con la promulgación de la Ley Orgánica de Protección de Datos Personales, aún enfrenta vacíos de implementación y control efectivo, especialmente en el ámbito laboral. La ley, inspirada en modelos europeos como el Reglamento General de Protección de Datos, establece principios robustos de juridicidad, finalidad, proporcionalidad y confidencialidad, pero su aplicación práctica se encuentra limitada por una débil institucionalidad y una escasa cultura de cumplimiento en los sectores público y privado.

Uno de los aspectos más debatidos es el consentimiento del trabajador en el uso de tecnologías biométricas para el control de asistencia. La relación de subordinación propia del vínculo laboral impide considerar el consentimiento como plenamente libre e informado, lo que genera un conflicto entre eficiencia empresarial y respeto a la autodeterminación informativa. La doctrina y la jurisprudencia internacional particularmente de la Agencia Española de Protección de Datos y el Comité Europeo de Protección de Datos coinciden en que el consentimiento en relaciones laborales es insuficiente como base jurídica, lo que exige fundamentos alternativos basados en la legalidad y la proporcionalidad del tratamiento.

Asimismo, se observa que el principio de legalidad opera como límite material al poder del empleador. Cualquier tratamiento de datos personales debe estar respaldado por una norma habilitante clara, con finalidad legítima, alcance definido y medidas de seguridad comprobables. En Ecuador, no existe disposición legal que obligue al uso de sistemas biométricos en el control laboral, lo que evidencia que su utilización responde a decisiones administrativas más que a mandatos normativos. Por tanto, la implementación de sistemas biométricos sin base legal específica podría configurarse como violatoria del derecho a la

autodeterminación informativa y del principio de proporcionalidad establecido en la Ley Orgánica de Protección de Datos Personales.

En el plano comparado, la legislación ecuatoriana mantiene una estructura alineada parcialmente con el Reglamento General de Protección de Datos europeo, aunque con menor grado de desarrollo técnico y sancionatorio. El modelo europeo impone mecanismos más rigurosos, como la privacidad desde el diseño, las evaluaciones de impacto obligatorias, y un régimen sancionador fuerte, aspectos que en Ecuador todavía están en proceso de consolidación. En contraste, la Ley chilena N.º 21.719, aunque reciente, presenta avances en materia institucional con la creación de una agencia autónoma de fiscalización quien vela por la privacidad de los ciudadanos, asegurando que las entidades públicas y privadas cumplan con la normativa siendo que sus funciones incluyen supervisar el manejo de datos personales, atender denuncias, ofrecer orientación y educación sobre derechos y deberes en privacidad, y desarrollar políticas y normativas para fortalecer la protección de la información personal en el país., mientras que la Superintendencia ecuatoriana aún enfrenta limitaciones operativas que afectan su capacidad de fiscalización efectiva.

Las normas internacionales de la OCDE, la ONU y la CIDH subrayan la importancia de conciliar el avance tecnológico con la protección de los derechos fundamentales, especialmente en situaciones de asimetría de poder como la relación laboral. En este sentido, Ecuador debería fortalecer su marco de evaluación de impacto, garantizar la independencia funcional de su autoridad de control y promover la educación cívica sobre los derechos de la ciudadanía en materia de protección de datos. El desconocimiento de los derechos por parte de los trabajadores impide el ejercicio efectivo de las garantías legales, lo que amplía la brecha entre el ejercicio formal y el ejercicio práctico de dichos derechos.

La consideración de los datos biométricos en el ámbito laboral ilustra la tensión entre el respeto a los derechos humanos y los avances del trabajo moderno. Si bien la Ley Orgánica de Protección de Datos Personales ha supuesto un avance en la construcción de un sistema de garantías regulatorias, su eficacia, dentro de un enfoque centrado en las garantías, se basa en el principio de legalidad, el funcionamiento de los controles institucionales y el desarrollo de un derecho a la privacidad integrado en la cultura de los derechos fundamentales. Solo mediante avances acordes con los tratados internacionales de derechos humanos y un estricto principio de necesidad y proporcionalidad se podrá evitar que la biometría en el trabajo se utilice como medio de control y vigilancia, y, en cambio, garantizar que sirva para respetar los derechos de los trabajadores.

Conclusiones

Los análisis realizados permiten concluir que en Ecuador existe una regulación legal limitada en materia de protección de los derechos relacionados con el uso de información biométrica en el ámbito laboral. Es necesario considerar tanto la formalización como el rigor del principio de legalidad. La promulgación de la Ley Orgánica de Protección de Datos Personales supone un avance en la protección de la privacidad y la autodeterminación informativa del ciudadano. Sin embargo, es preciso recalcar que se trata de un avance y no de una solución definitiva, dado que la legislación no es plenamente aplicable debido a la ausencia de una defensa normativa sustantiva, un marco institucional limitado y una escasa preocupación social por el ejercicio de este derecho.

La comprensión que aporta la investigación sobre la clasificación de la información biométrica es clara. La información biométrica no es información cualquiera; describe e identifica a una persona y, potencialmente, captura parte de su capital humano. La falta de control y regulación de los derechos de los usuarios en la aplicación de las tecnologías biométricas puede provocar consecuencias irreparables en materia de privacidad, libertad y dignidad humana. El uso de la biometría por parte del empleador para controlar el comportamiento y los procesos laborales de los empleados requiere una justificación legal, y los datos utilizados para lograr dicho propósito deben ser los menos intrusivos. En Ecuador, la ley de protección de datos es aún relativamente reciente y débil.

El estudio demuestra que el principio de legalidad no solo actúa como un requisito formal, sino también como un límite sustantivo al poder de decisión del empleador. Todo tratamiento de datos, especialmente de datos biométricos, debe estar respaldado por una norma habilitante que establezca claramente los fines, los responsables, el plazo de conservación y las garantías para el titular de los datos. Sin este fundamento jurídico, la recopilación de datos biométricos en el lugar de

trabajo es inválida y, por lo tanto, ilegal, lo que afecta al derecho constitucional de las personas a controlar sus datos personales.

El análisis comparativo de la normativa ecuatoriana frente al Reglamento General de Protección de Datos de la Unión Europea y otras legislaciones de América Latina permite concluir que la normativa ecuatoriana defiende los mismos principios fundamentales: legalidad, transparencia, proporcionalidad y rendición de cuentas proactiva. Sin embargo, en materia de prevención, establecimiento de sanciones y cooperación internacional, el marco legislativo de la Unión Europea es más sólido, y el modelo ecuatoriano aún necesita fortalecer su marco institucional.

Bibliografía

Agencia Española de Protección de Datos (AEPD). (2022). *Evaluación de tecnologías biométricas desde la perspectiva de la protección de datos*. Recuperado de https://www.aepd.es/es/prensa-y-comunicacion/blog/biometric-data-assessment-from-a-data-protection-perspective

Aguiar, R. M. (2017). *Derechos fundamentales y relaciones laborales*. Editorial Dykinson.

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449 de 20 de octubre de 2008.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459 de 26 de mayo de 2021.

Asamblea Nacional del Ecuador. (2023). *Reglamento de la Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 435 de 13 de noviembre de 2023.

Atienza, M. (2006). *El sentido del derecho*. Ariel.

Barreiro González, L. (2019). *La protección de datos personales en las relaciones laborales: límites y garantías*. Revista de Derecho Laboral y Seguridad Social, 35(2), 113–131.

Carbonell, M. (2021). *Derecho constitucional y derechos fundamentales* (2.ª ed.). Editorial Tirant lo Blanch.

Carbonell, M. (2021). *Derechos fundamentales en la era digital*. Tirant lo Blanch.

Carpizo, J. (1999). *Estudios constitucionales*. Editorial Porrúa.

CIDH - Relatoría Especial para la Libertad de Expresión. (2021). *Declaración conjunta sobre libertad de expresión y vigilancia de los usuarios en internet*. OEA.

Comisión Interamericana de Derechos Humanos (CIDH). (2017). *Estándares interamericanos sobre protección de datos personales: aprobación de los Principios sobre privacidad y protección de datos personales*. Organización de los Estados Americanos. Disponible en: https://www.oas.org/es/cidh/expresion/

Comisión Interamericana de Derechos Humanos (CIDH). (2017). *Principios sobre privacidad y protección de datos personales*.

Comité Europeo de Protección de Datos (Artículo 29 Working Party). (2011). *Opinion 15/2011 on the definition of consent*. Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Comité Europeo de Protección de Datos. (2020). *Directrices sobre el consentimiento conforme al RGPD*. https://edpb.europa.eu

Congreso Nacional de Chile. (1999). *Ley N.º 19.628 sobre Protección de la Vida Privada*. Diario Oficial de la República de Chile.

Consejo de Europa. (1981). *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* (Convenio 108).

Contreras, P. (2020). *El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena.* Estudios constitucionales vol.18 no.2 Santiago.

Cordero, E. (2019). *Protección de datos personales en Chile: evolución, desafíos y propuestas de reforma*. Revista de Derecho Público, (91), 45-67.

Corte Constitucional del Ecuador. (2015). *Sentencia No. 182-15-SEP-CC*.

Corte Constitucional del Ecuador. (2021). Sentencia No. 13-18-CN/21. Recuperado de https://jurisprudencia.corteconstitucional.gob.ec

Cotino Hueso, L. (2019). *Derechos fundamentales y protección de datos: hacia un nuevo modelo de garantías*. Tirant lo Blanch.

Cuomo, G. (2015). *Biometría y derechos fundamentales en la era digital*. Editorial Tirant lo Blanch.

Danesi, C. (2020). *Datos personales y decisiones automatizadas*. Editorial Tirant lo Blanch.

De Hert, P., & Papakonstantinou, V. (2018). *Data Protection and Privacy: The Age of Intelligent Machines*. Hart Publishing.

Domingo, V. (2017). *Protección de datos personales y responsabilidad proactiva*. Editorial Tirant lo Blanch.

European Data Protection Board. (2020). *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)*. https://edpb.europa.eu

European Data Protection Board. (2021). *Guidelines 05/2021 on Data Protection Impact Assessment (DPIA)*. EDPB.

Ferrajoli, L. (2001). *Derecho y razón: Teoría del garantismo penal*. Trotta.

Fonseca, F. (2019). *Protección de datos personales: Fundamentos jurídicos y retos regulatorios*. Tirant lo Blanch.

Fuentes, J. (2021). *Hacia una autoridad de protección de datos en Chile: retos y perspectivas*. Anuario de Derecho Público, 8(1), 213-234.

GADISA. (2023). *Análisis sobre la adecuación de la normativa ecuatoriana a estándares internacionales de protección de datos personales*. Quito: Grupo Andino de Derecho Informático y Sociedad Abierta. [Documento técnico interno].

García Amado, J. A. (2018). *Derecho y datos personales: elementos para una teoría garantista*. Editorial Tecnos.

García Mexía, P. (2013). *Protección de datos personales y garantía de derechos*. Aranzadi.

García, S. (2015). *Interpretación constitucional y derechos fundamentales*. Editorial Porrúa.

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press.

International Association of Privacy Professionals. (2023). *Global privacy enforcement and harmonization: Challenges and best practices*. https://iapp.org/resources/article/global-privacy-enforcement-and-harmonization-challenges-and-best-practices/

Kuner, C. (2017). *The General Data Protection Regulation: A Commentary*. Oxford University Press.

López Álvarez, M. (2018). *Consentimiento y poder en el ámbito laboral*. Revista de Derecho Social, (83), 125-138.

Lozano, G. (2020). *Privacidad del trabajador y control empresarial*. Editorial Porrúa.

Martínez García, A. (1 de agosto 2025). *La inteligencia artificial en la empresa tiene límites: Los derechos no se pueden automatizar*. Cinco Días – El País. https://cincodias.elpais.com/legal/2025-08-01/la-inteligencia-artificial-en-la-empresa-tiene-limites-los-derechos-no-se-pueden-automatizar.html

Martínez Martínez, R. (2004). *Una aproximación crítica a la autodeterminación informativa*. Quito: Ediciones CEDIS.

Murillo Garzón, V. (2021). *Evaluación de impacto y tratamiento de datos sensibles*. Revista Latinoamericana de Protección de Datos, 2(1), 85–97.

Naciones Unidas (ONU). (2018). *Declaración Conjunta sobre Libertad de Expresión y Privacidad*. Relatoría Especial de la ONU sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión. Disponible en: https://www.ohchr.org

Organización de las Naciones Unidas (ONU), Organización de los Estados Americanos (OEA), Organización para la Seguridad y la Cooperación en Europa (OSCE), & Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). (2018). *Declaración conjunta sobre libertad de expresión y privacidad*. https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1101&IID=2

Organización de las Naciones Unidas (ONU). (2013). *Resolución sobre la Protección de la Privacidad en el Contexto de la Vigilancia y la Interferencia en las Comunicaciones*.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2013). *Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales* (actualización de 1980). OCDE Publishing.

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Pavez, M. (2020). *Privacidad y datos personales en el ordenamiento chileno: una visión comparada*. Editorial Jurídica de Chile.

Pavez, M. (2020). *Privacidad y datos personales en el ordenamiento chileno: una visión comparada*. Editorial Jurídica de Chile.

Pérez Asinari, M. (2022). *Protección de datos biométricos: desafíos regulatorios y garantías para los titulares*. Revista Iberoamericana de Protección de Datos Personales, 8(1), 45–68.

Pollicino, O., & Romeo, G. (2020). *Protección de datos y derechos fundamentales: una visión comparada entre Europa y América Latina*. Ediciones Jurídicas Cuyo.

Puyol Montero, E. (2013). *Autodeterminación informativa y principio de finalidad*. Revista de Derecho y Nuevas Tecnologías, 9, 41–58.

Red Iberoamericana de Protección de Datos. (2021). *Guía para la protección de datos personales en el ámbito laboral*. Disponible en: https://www.redipd.org

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (27 de abril de 2016). *Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)*. Diario Oficial de la Unión Europea, L 119.

Relatoría Especial para la Libertad de Expresión de la CIDH. (2021). *Informe anual sobre libertad de expresión*. Capítulo sobre protección de datos y tecnologías de vigilancia. Organización de los Estados Americanos. Disponible en: https://www.oas.org/es/cidh/expresion/informes/anuales.asp

Reyes Amán, J. G. (2016). *Derecho a la protección de datos personales en las bases de datos judiciales accesibles al público en temas de niñez y adolescencia* [Trabajo de titulación, Universidad de las Américas]. Repositorio Institucional UDLA. https://repositorio.udla.edu.ec/handle/33000/5310

Rodríguez López, A. (2020). *Transición entre reconocimiento y realización efectiva de derechos*. *Revista Latinoamericana de Derechos Humanos, 12*(2), 65–82.

Rodríguez, M. (2018). *Institucionalidad y protección de datos*. Editorial Tirant lo Blanch.

Rodríguez, M., & Castañeda, L. (2020). *Protección de datos personales en Ecuador: avances y desafíos*. Revista Jurídica Latinoamericana, 8(2), 45-67.

Roldán Carrillo, F. N. (2022). *Los ejes centrales de la protección de datos: consentimiento y finalidad*. *USFQ Law Review, 8*(1), 25–42. https://doi.org/10.18272/ulr.v8i1.2184

Rosas, G & Cardenas, G. (2023). *LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR Una revisión histórica-normativa de este derecho fundamental en el país suramericano*.

Rubio Llorente, F. (2006). *Derechos fundamentales, derechos humanos y Estado de Derecho*. Universidad de Oviedo, p. 5.

Sánchez Esparza, I. (2023, febrero 9). *La privacidad desde el diseño: nuevo estándar*. KPMG Tendencias.

Sánchez-Castañeda, A., & Márquez, J. (2019). *Tratamiento de datos personales y acceso a la información*. Revista Digital Jurídica, Estado de derecho y protección de datos. Redalyc.

Serra, M. M. (2001). *El Habeas Data en el Derecho Argentino*. Juris.

Superintendencia de Protección de Datos Personales. (2025). Consulta 2025-0031-O — Biometría en el control de asistencia laboral. Quito, SPDP.

Tribunal Constitucional Español. (2000). *Sentencia 292/2000, de 30 de noviembre de 2000*. Boletín Oficial del Estado.

Troncoso Reigada, A. (2012). *La protección de datos personales en el Derecho español*. Editorial Dykinson.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Anexos

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Mateo Josue Carchipulla Fajardo, portador(a) de la cédula de ciudadanía Nº **0150051399,** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación " **El tratamiento de datos personales biométricos dentro de entornos laborales en el marco de la Ley Orgánica de Protección de Datos Personales frente al principio de legalidad"** Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, 28 de noviembre del 2025

F: .....

Mateo Josue Carchipulla Fajardo

C.I 0150051399