

<https://doi.org/10.69639/arandu.v12i3.1583>

Tratamiento de datos biométricos laborales: consentimiento vs. derechos fundamentales en Ecuador

Processing of Biometric Labor Data: Consent vs. Fundamental Rights in Ecuador

Marlon Joey Pallo Quimbíta

mpallo3@indoamerica.ed.ec

<https://orcid.org/0009-0000-9669-4278>

Facultad de Jurisprudencia y Ciencias Políticas

Carrera de Derecho

Universidad Tecnológica Indoamerica

Alfredo Fabián Carrillo

alfredocarrillo@uti.edu.ec

<https://orcid.org/0000-0001-5197-8760>

Universidad Tecnológica Indoamérica

Ambato, Ecuador

Artículo recibido: 18 agosto 2025 - Aceptado para publicación: 28 septiembre 2025

Conflictos de intereses: Ninguno que declarar.

RESUMEN

Este estudio se enfoca en el estudio del tratamiento de datos biométricos laborales, específicamente consentimiento vs. derechos fundamentales en Ecuador. El objetivo es analizar la aplicación de estos datos y la manera en que puede afectar los derechos fundamentales como a la intimidad y la dignidad, de no existir consentimiento para ello. Igualmente, se revisa el concepto de dato biométrico, su evolución, el marco normativo nacional e internacional en materia de derechos humanos, los principios que lo rigen al igual que al Derecho Laboral, se analiza el derecho al trabajo y una vida digna. Ello se lleva a cabo mediante una metodología cualitativa, empleando la técnica bibliografía documental y métodos como el exegético jurídico y analítico sintético, entre otros. Se concluye que, aun cuando los datos biométricos generan eficiencia en el entorno laboral ecuatoriano, su uso plantea riesgos jurídicos importantes debido a la falta de consentimiento libre y a la desigualdad de poder. Esto afecta derechos fundamentales y exige control, supervisión efectiva y garantías reales para proteger la intimidad y dignidad del trabajador.

Palabras Clave: consentimiento, datos biométricos, derechos fundamentales, derecho laboral

ABSTRACT

This study focuses on the processing of biometric data in the workplace, specifically examining consent versus fundamental rights in Ecuador. The objective is to analyze the use of such data and how it may affect fundamental rights such as privacy and human dignity. To achieve this, the

research reviews the concept of biometric data, its evolution, the national and international legal frameworks on human rights, the governing principles, alongside labor law and examines the right to work and to a dignified life. The study uses a qualitative methodology, employing documentary bibliographic techniques and legal exegesis and analytical-synthetic methods, among others. The conclusion indicates that although biometric data enhances efficiency and security in Ecuador's labor context, its use raises ethical and legal dilemmas due to insufficient consent mechanisms and power imbalances, which jeopardize the exercise of fundamental rights and call for effective protection.

Keywords: consent, biometric data, fundamental rights, labor law

Todo el contenido de la Revista Científica Internacional Arandu UTIC publicado en este sitio está disponible bajo licencia Creative Commons Attribution 4.0 International. 

INTRODUCCIÓN

Esta investigación se enfoca en el estudio del tratamiento de datos biométricos laborales: consentimiento vs. derechos fundamentales en Ecuador. Para contextualizar el estudio es necesario exponer que, en siglos anteriores, la protección jurídica de las libertades individuales y la privacidad era prácticamente inexistente. Por ello, estos valores no se contemplaban en los marcos normativos ni en la conciencia social. Sin embargo, con el desarrollo paulatino de la definición de libertad individual y el reconocimiento de los derechos fundamentales, tal como analiza Rodríguez (2019), la idea de privacidad comenzó a relacionarse con la dignidad humana, lo que condujo a que fuera objeto de tutela legal. Este proceso, en Ecuador se contempló en la Constitución de 1998 y, se reguló, de manera más completa, en la Constitución vigente.

Lo anterior, permitió la positivización de derechos fundamentales vinculados de índole íntima y personal de las personas, entre ellos, la protección de datos y la privacidad en el ámbito laboral. Este desarrollo histórico y normativo expone una transición desde la ausencia de garantías, hacia un sistema jurídico que reconoce y protege la información personal de los trabajadores, de conformidad con instrumentos internacionales de derechos humanos y las actuales constituciones.

En ese marco, con el transcurso del tiempo y con la introducción de las innovaciones tecnológicas y digitales, han aparecido los datos biométricos. Estos como analiza Mercader (2020) comprenden información única e intransferible como huellas digitales dactilares, reconocimiento facial, patrones de iris o de voz, los que se emplean para el control de asistencias, identificación y seguridad en los entornos de trabajo. Dicha información debe ser objeto de salvaguarda por su importancia en todos los ámbitos, entre ellos, el laboral.

Como se ha expuesto, muchas empresas, han puesto en práctica los sistemas biométricos como un mecanismo para asegurar su eficiencia operativa. Sin embargo, su empleo saca a la luz problemáticas éticas y jurídicas en relación con la protección de los derechos fundamentales, especialmente el derecho a la privacidad, intimidad al igual que otras cuestiones vinculadas al consentimiento para su uso y la dignidad del trabajador.

En Ecuador, el ordenamiento jurídico regula la protección de datos personales mediante normativas como la Ley Orgánica de Protección de Datos Personales, que prevé la utilización de estos, clasifica los datos biométricos como datos sensibles. Sin embargo, aún existe incertidumbre acerca de la aplicación efectiva de esta normativa en contextos laborales, lo que cuestiona la validez del consentimiento otorgado para el uso de ellos.

En ese sentido, se han desarrollado en el país varias investigaciones enfocadas en el asunto antes descrito, Aguirre (2023) estudió el tema “Uso de datos biométricos (biometría) como método para aceptar las políticas de uso de datos personales”. Entre sus objetivos están analizar el uso de datos biométricos para aceptar políticas de uso de datos personales en plataformas

digitales bajo la legislación ecuatoriana y evaluar la biometría como mecanismo de seguridad para garantizar un consentimiento informado y auténtico. Además, proponer la biometría como alternativa para fortalecer la protección de datos personales y reducir los riesgos de suplantación de identidad y acceso no autorizado.

Al respecto, Aguirre (2023) aplicó en el estudio mencionado, un enfoque jurídico-doctrinal y comparativo. En este se concluyó que la salvaguarda de los datos personales es un derecho fundamental reconocido en el país y que el consentimiento informado es fundamental para asegurar su tratamiento legítimo. Igualmente, que la biometría, aun cuando presenta sus riesgos, perfecciona la autenticación y puede reconocerse legalmente como un método que expresa el consentimiento digital, consolida la seguridad y la precautela la privacidad de las personas.

Por otro lado, Villa et al. (2024) desarrollaron el tema “Protección de Datos Personales en Ecuador y Colombia: Principios, Ética y Desafíos Actuales”, sus objetivos se enfocaron en analizar el concepto de protección de datos personales y su tratamiento en Ecuador y Colombia, en particular, los principios que deben regir dicho proceso, como la legalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad. En esta investigación se empleó una metodología sustentada en la revisión doctrinal y en un derecho comparado. Igualmente se examinaron casos prácticos acerca de la recopilación de información sobre el uso de datos biométricos. Este concluyó en que el tratamiento de los datos de los individuos constituye una gran responsabilidad y exige su manejo correcto, en caso contrario, puede generar consecuencias legales y éticas. Por esto se deben aplicar los principios que corresponden y distinguir entre aquella información que se emplea en el marco público y privado, para asegurar la seguridad y confidencialidad de la información.

Asimismo, Borbor y Chaca (2024) estudiaron el tema del “Consentimiento en el uso de datos sensibles y la Ley Orgánica de Protección de Datos Personales en el ámbito privado”. El objetivo general se enfocó en analizar los componentes del consentimiento en el tratamiento de datos personales. La investigación destaca la importancia de cumplir con esta formalidad y la frecuente vulneración de la privacidad en que incurren las empresas al suscribir contratos y no observar los requisitos en cuanto a la obtención de la autorización de sus clientes, lo que constituye un incumplimiento de la normativa vigente en la materia. El trabajo se desarrolló mediante una metodología mixta que unió el análisis normativo, doctrinal y la aplicación de encuestas. Este arroja como conclusión que la norma antes referida, se aplica de manera insuficiente y coloca a los individuos en una situación vulnerable ante el uso ilegítimo de su información sensible.

En virtud de lo anterior, se aprecia que, en Ecuador, la academia ha estudiado el tema de la protección de datos personales, los que servirán de base a este artículo. Sin embargo, la relevancia de este trabajo está en que analiza el tratamiento de los datos biométricos en el contexto laboral para definir lo concerniente al consentimiento contra los derechos fundamentales a partir de las

violaciones que les puede generar a estos. Esta investigación es de gran valor porque su propósito es proteger los derechos constitucionales y beneficiar a las personas y la sociedad en general.

Por lo expuesto, este artículo tiene como objetivo analizar la aplicación de estos datos y la manera en que puede afectar los derechos fundamentales como a la intimidad y la dignidad, de no existir consentimiento para ello.

DESARROLLO

Evolución del concepto de datos biométricos y su naturaleza en el ámbito laboral

Para contextualizar el tema de estudio es necesario referirse a la evolución que han manifestado los datos biométricos hasta llegar a su aplicación actual en el ámbito laboral. Para ello se debe exponer que los datos biométricos, guardan relación directa con la identidad biológica única de cada ser humano, a respecto se afirma que:

El concepto de biometría proviene de las palabras bio (vida) y metría (medida) lo que significa que los sistemas o equipos biométricos miden e identifican alguna característica propia, tanto física como de comportamiento de una persona. Esto ha dado pie a utilizar estas mediciones como metodologías de seguridad que permiten el reconocimiento de características físicas intransferibles de las personas para su identificación (Ruiz et al., 2009,p.30)

Bajo esta definición, se debe exponer que la aplicación de la biometría ha conllevado para Mercader (2023) a un cambio desde métodos básicos de identificación hasta sofisticados sistemas automatizados capaces de identificar personas con alta exactitud. En sus inicios, la biometría se fundamentaba en la observación y documentación manual de rasgos físicos perceptibles, tales como cicatrices o señales corporales, empleadas en antiguas civilizaciones para identificar a los individuos en comunidades reducidas.

No obstante, el mayor progreso científico tuvo lugar en el siglo XIX, cuando la identificación personal se convirtió en una disciplina metódica y cuantificable, estableciendo la base para la evolución futura de tecnologías biométricas. Según Jain et al.(2017) la biometría, se considera la identificación automática de personas basándose en características físicas o conductuales, lo que tiene un origen histórico lejano. Sin embargo, su desarrollo como disciplina científica se produjo con la antropometría de Alphonse Bertillon. Este procedimiento, implicaba la medición de dimensiones concretas del cuerpo humano, como la longitud del antebrazo o el diámetro de la cabeza, con el fin de construir un perfil singular de cada individuo. Este método fue adoptado ampliamente por las fuerzas policiales europeas y estadounidenses, lo que marcó el inicio de la biometría moderna y demostró la viabilidad de la identificación basada en características físicas objetivas.

En ese orden, como explica Escajedo (2017) destaca la figura de Francis Galton el que transformó el mundo de la biometría, al evidenciar la singularidad de las huellas dactilares, lo que

propició su amplia adopción en el proceso de identificación forense y policial. Luego, Edward Henry amplió este esfuerzo al desarrollar un sistema de categorización de dichas huellas que simplificó la administración de grandes bases de datos, posibilitando la identificación inmediata de personas. Este progreso dio lugar a que se considere la huella dactilar como la norma mundial para la identificación individual durante gran parte del siglo XX.

Luego en el siglo XX, la biometría expandió su campo de acción con la inclusión de nuevas variantes. Según Jain et al. (2017), indican que, aparte de las huellas dactilares, se comenzaron a emplear rasgos como el iris, la voz, la geometría de la mano y la firma manuscrita, lo que amplió su aplicación a otros campos más allá del policial. Estas técnicas posibilitaron su puesta en práctica en la regulación de accesos, la comprobación de identidad en servicios bancarios y la administración de fronteras, lo que demostró su flexibilidad y capacidad de adaptación a contextos civiles y comerciales.

En esa línea, la automatización de los sistemas biométricos, desde la segunda parte del siglo XX, como afirma Mercader (2023) se comenzó a utilizar en el entorno laboral. Esto a partir de que, desde los años 60, la evolución de algoritmos para el reconocimiento facial y de voz posibilitó la construcción de sistemas que podían cotejar patrones biométricos con bases de datos electrónicas de forma eficaz, simplificando el control de acceso y la administración de asistencia en centros laborales. Ello transformó la biometría en un instrumento enfocado en la seguridad y la gestión de recursos humanos, lo que facilitó la identificación a gran escala y el registro del horario de trabajo en fábricas, oficinas y organismos gubernamentales.

Por tanto, en la actualidad, la incorporación de sistemas multimodales que fusionan las características biométricas como huellas dactilares, identificación facial e iris, ha permitido con exactitud los controles de acceso en el ámbito del trabajo. Estos sistemas, al exigir que varios parámetros biométricos coincidan para permitir el ingreso o documentar la asistencia, como explica Escajedo (2017) han disminuido los errores y ha aumentado la seguridad ante intentos de fraude de identidad. Su aplicación es importante en áreas donde la salvaguarda de datos o bienes es fundamental lo que ha reconocido a la biometría como un referente en la administración de los recursos humanos.

Cabe mencionar que para Rodríguez (2019) los datos biométricos al permitir, identificar a la persona y contener información de naturaleza íntima como problemas de tipo genético o condiciones de salud, exige que, al ser utilizados, se respete el derecho a la intimidad bajo los principios de equidad, proporcionalidad y legalidad. Además, el consentimiento voluntario por parte del trabajador es necesario para que estos, se consideren válidos y deben respetarse, aun cuando existe un desequilibrio de poder en la relación laboral.

Marco normativo del tratamiento de datos personales y biométricos en el Ecuador

Para estudiar el tratamiento de datos personales y biométricos en el ordenamiento jurídico ecuatoriano, se debe partir de que, como prevé el artículo 417 de la Constitución de la República

del Ecuador (2008), los tratados internacionales que han sido objeto de ratificación por el país en materia de derechos humanos se aplicarán de manera directa y justamente, el tratamiento de datos personales y biométricos al igual que su protección tienen su base en el derecho humano a la intimidad.

Por lo anterior, se debe iniciar por mencionar que la Declaración Universal de Derechos Humanos (1948) es la primera disposición jurídica que reconoció al derecho a la intimidad como un derecho humano, tal como prevé en el artículo 12. Este dispone que ninguna persona puede sufrir injerencias arbitrarias o ilegales en su vida privada, ni ninguna clase de ataques ilegítimos a su honra y reputación. Además, que posee el derecho a la protección por parte de la ley ante este tipo de intervención.

Del mismo modo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966) reconoce el derecho a la intimidad de las personas. Asimismo, la Convención Americana sobre Derechos Humanos (1969) en el artículo 11 prevé el referido derecho a partir del respeto a la honra y a la dignidad humana. A partir de ello, se consagra que “nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia” (p.7).

En ese marco, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos mediante la Observación General No 16 sobre el derecho a la intimidad (1988) indica que los Estados son los responsables de asegurar que la vida privada, el honor y la reputación de las personas estén salvaguardada frente a cualquier injerencia o uso indebido de su información personal, ya sea por parte de autoridades públicas o entidades privadas.

Igualmente, la Observación (1988) mencionada, prevé que la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos deben estar regulados por la normativa interna. Además, que están obligados a adoptar medidas para evitar que la información sobre la vida privada de las personas se utilice para fines incompatibles con el respeto a los derechos humanos, y para garantizar que los individuos puedan acceder, rectificar o eliminar sus datos personales almacenados de forma incorrecta o ilegal.

Lo antes expuesto, guarda relación con la gestión de los datos biométricos en el entorno laboral, ya que exige que, el tratamiento de este tipo de información esté debidamente justificado, regulado y pueda ser objeto de controles de seguridad y transparencia. Como se aprecia el derecho a la intimidad está contemplado en instrumentos internacionales de derechos humanos, lo que obliga a su observancia en todos los contextos al ser un derecho humano.

En consonancia con lo anterior, la Constitución de la República del Ecuador (2008) en el artículo 66 numeral 19, reconoce el derecho a la protección de datos personales que comprende el poder acceder y decidir en relación con la información y los datos de esta naturaleza al igual que su salvaguarda. Al respecto prevé que tanto su recolección como el archivo, su procesamiento, distribución o divulgación deben ser autorizados por el titular o debe existir una regulación

jurídica que lo ampare. Asimismo, en el artículo 20 consagra el derecho a la intimidad del que es titular toda persona.

En virtud de las regulaciones constitucionales expuestas, en Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD) (2021). Esta en el artículo 1, reconoce como su objetivo, garantizar el derecho de todas las personas a la protección de sus datos personales, permitiendo el acceso, control y decisión sobre esa información. Asimismo, contempla principios, derechos, obligaciones y mecanismos de tutela que buscan asegurar un manejo responsable y transparente de los datos personales, aplicables al sector público y privado.

En cuanto al ámbito material de aplicación, la LOPD (2021) en el artículo 2 prevé que esta norma rige sobre cualquier tratamiento de datos personales, que esté en soporte físico o digital, automatizado o no, y en cualquier modalidad de uso posterior, excluyendo actividades familiares, datos anonimizados, actividades periodísticas, ciertos datos regulados por normativas especializadas y los datos de personas jurídicas, entre otros casos específicos.

Igualmente, la LOPD (2021), en el artículo 4, define los términos consentimiento y dato biométrico. El primero lo reconoce como expresión de la decisión libre, concreta, informada e incuestionable, por la que el propietario de los datos personales autoriza al encargado del tratamiento de dicha información a gestionarlos. Por su lado, el segundo se considera la información de tipo personal y única, relacionada con las propiedades físicas o fisiológicas, o comportamientos de un individuo que facilite o verifique la identificación exclusiva de este como fotografías faciales o datos dactiloscópicos, entre otros.

Del mismo modo, en el antes referido artículo 4 de la Ley (2021), se reconocen dentro de los datos relativos a los biométricos al igual que se enmarcan en los datos sensibles. Con respecto a estos últimos, como regula el artículo 25 de esta norma se ubican en la categoría de datos personales especiales, lo que exige un tratamiento especial de acuerdo al artículo 26 que se tratará más adelante. Asimismo, como prevé el artículo 92 del texto constitucional (2008) su archivo debe contar con autorización de la ley o por parte de la persona titular, además debe contar con las medidas de seguridad necesarias. En caso de no responder a ello, se puede acudir a un órgano constitucional a demandar los perjuicios ocasionados.

Por otra parte, el artículo 7 de la Ley examinada (2021) prevé los requisitos para el tratamiento legítimo de los datos personales. Entre ellas, destaca el consentimiento expreso del titular para fines específicos; el cumplimiento de una obligación legal por parte del responsable; una orden judicial; la realización de una misión en interés público o en ejercicio de poderes públicos; la ejecución de medidas precontractuales o contractuales; la protección de intereses vitales como la vida o la salud; el uso de datos provenientes de bases de acceso público, o la existencia de un interés legítimo del responsable o de un tercero, siempre que no prevalezcan los derechos fundamentales del titular.

Asimismo, se debe hacer mención del artículo 8 de la Ley Orgánica de Protección de Datos Personales (2021) dispone sobre el consentimiento. Al respecto regula que podrá dar tratamiento y comunicar en relación con los datos personales cuando exista una manifestación de la voluntad por parte del titular para ello. Asimismo, exige que dicho consentimiento cumpla con los siguientes requisitos:

1. **Libre:** ello implica que el consentimiento no este viciado.
2. **Específica:** a partir de que debe definir de manera concreta los medios y la finalidad del tratamiento de los datos.
3. Informada; debe responder al principio de transparencia y asegurar el derecho a la transparencia.
4. **Inequívoca:** exige que no exista incertidumbre alguna en relación con el alcance de la autorización concedida por su titular.

Además, se dispone en dicho artículo, que el consentimiento puede ser objeto de revocación en cualquier momento sin que medie justificación alguna. Esto debe ser aplicado sustentado en un procedimiento simple, dotado de eficiencia, celeridad, gratis y eficaz. Como se aprecia, estos requerimientos aseguran que el manejo de los datos personales sea transparente, justificado y respetuoso de los derechos fundamentales de las personas. De esta manera, la norma salvaguarda a los titulares frente a usos indebidos o excesivos de su información personal, por lo que debe constar una justificación para cualquier tratamiento de datos.

Por otro lado, la Ley (2021) reconoce entre los artículos 12 y 24 un grupo de derechos para los titulares de datos que resultan aplicables al contexto laboral. El primero, es el derecho a la información, que asegura que toda persona debe ser informada de manera clara y transparente sobre los fines, la base legal, el tiempo de conservación, el responsable del tratamiento, las transferencias de datos y las consecuencias de entregar o no sus datos, entre otros aspectos. Igualmente está el derecho de acceso, que permite a los titulares, conocer y obtener gratuitamente toda la información que se tenga sobre ellos. Asimismo, prevé el derecho de rectificación y actualización de datos inexactos o incompletos al igual que el derecho de eliminación, que permite solicitar la supresión de datos cuando ya no sean necesarios, se haya revocado el consentimiento o se afecten derechos fundamentales.

También, la LOPDP (2021) consagra el derecho de oposición, que permite negarse a ciertos tratamientos de datos, en particular, en casos de mercadotecnia directa o cuando existan motivos personales justificados. El derecho a la portabilidad es otro de los contemplados en la norma y permite al titular solicitar la transferencia de sus datos a otros responsables en formatos compatibles y de lectura mecánica. Además, está el derecho a la suspensión del tratamiento en situaciones específicas, y el derecho a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas, este permite solicitar explicaciones y presentar observaciones.

Finalmente, el artículo 22 de la Ley estudiada (2021) otorga el derecho de consulta pública y gratuita sobre el registro de datos personales, y el derecho a la educación digital para promover el uso responsable y seguro de la información personal. Todos estos derechos son irrenunciables y su ejercicio debe ser facilitado por los responsables del tratamiento para asegurar la protección de la privacidad y la autodeterminación informativa en el entorno digital.

Por otra parte, es necesario exponer que el artículo 26 de la LOPDP (2021) regula el tratamiento de datos sensibles, dentro de los que están los datos biométricos. Al respecto, se prohíbe, como regla general, el tratamiento de datos personales sensibles, salvo en situaciones excepcionales. Este tratamiento solo se permite, si el titular otorga un consentimiento explícito y específico para fines determinados, o si resulta indispensable para cumplir obligaciones o ejercer derechos en el ámbito laboral, de la seguridad social o la protección social. También, cuando sea necesario para salvaguardar intereses vitales del titular o de otra persona natural, especialmente si el titular no puede dar su consentimiento por razones físicas o legales.

Otras excepciones previstas en el artículo 26 de la referida Ley (2021), incluyen los casos en que los datos sensibles hayan sido hechos públicos de manera manifiesta por su titular, cuando exista una orden judicial que lo autorice, o si el tratamiento tiene fines de archivo en interés público, investigación científica, histórica o estadística, respetando las medidas específicas de protección y proporcionalidad. Finalmente, el tratamiento de datos de salud estará sujeto a las disposiciones particulares de la ley. En todos los supuestos, la protección de los derechos y la privacidad del titular debe ser prioritaria, y cualquier excepción debe estar debidamente justificada y sujeta a controles estrictos.

Por otro lado, está el Reglamento General de la Ley Orgánica de Protección de Datos Personales (2023) tiene como objeto de conformidad con el artículo 1 desarrollar la normativa para la aplicación de la LOPD. Además, su ámbito de aplicación de acuerdo a lo dispuesto en el artículo 2, comprende a todas las personas naturales y jurídicas, nacionales y extranjeras, del sector público y privado, que realicen tratamiento de datos personales, en el contexto de que sus actividades como responsable o encargado de tratamiento de datos personales, tenga lugar en el territorio ecuatoriano o no.

En relación con el consentimiento el artículo 5 del Reglamento (2023) establece que el consentimiento del titular es un requisito primordial y debe obtenerse de forma explícita, previa e informada, siempre que la Ley lo exija para tratar sus datos personales. El responsable está obligado a explicar claramente las finalidades del tratamiento, el tiempo de conservación, las medidas de protección y las consecuencias de entregar los datos, asegurando que la persona otorgue su autorización mediante una acción afirmativa clara. Este consentimiento debe ser verificable ante la autoridad competente. Además, dispone que el silencio o la falta de respuesta del titular no se considerarán una forma válida de consentimiento.

Tal como se ha expuesto, las normativas nacionales e internacionales en materia de protección de datos personales, se aplican a aquellos de naturaleza biométrica que se utilizan en el ámbito laboral, lo que exige su protección. Igualmente, estas disposiciones representan una garantía para que se haga empleo de las innovaciones tecnológicas de manera equilibrada con la salvaguarda de los derechos fundamentales. Esto obliga a los empleadores a adoptar prácticas transparentes, que aseguren que el empleo de datos biométricos sea justificado, seguro y apegado a derecho.

Principios y derechos fundamentales en el contexto laboral

De acuerdo con Dworkin (2014), los principios en derecho son reglas fundamentales cuyo acatamiento satisface demandas de justicia, equidad y valores éticos, más allá de intereses políticos, sociales o económicos. Entre los principios que rigen el Derecho Laboral, está el principio protector que nace de la necesidad de equilibrar la relación entre empleador y trabajador, que manifiesta desequilibrio de poder. Este se fundamenta en la libertad de contratación, pero reconoce que esta, no asegura una igualdad real entre las partes, por lo que el ordenamiento jurídico determina mecanismos de protección para garantizar condiciones laborales justas y favorables para el empleado (Plá, 2016).

Por otra parte, está el principio de la norma más favorable que en entorno laboral establece que, cuando existen varias normativas aplicables a un mismo caso, el juez debe aplicar a la que otorgue mayores beneficios al trabajador, incluso si se trata de una disposición de menor jerarquía normativa. Alonso y Casas (2017), explican que este principio implica dejar de lado los criterios tradicionales de especialidad y jerarquía para priorizar la protección jurídica del empleado, para garantizar que siempre prevalezca la opción más ventajosa para él.

También, como analiza Palavecino (2020) este principio se fundamenta en la naturaleza progresiva de las garantías laborales, donde las normas superiores fijan estándares mínimos y las inferiores pueden ampliarlos, pero nunca reducirlos. Así, la aplicación de la norma más favorable no supone la derogación de las leyes de mayor rango, sino que permite elegir, entre normas de igual o diferente jerarquía, la que brinde mejores condiciones al trabajador.

Otro de los principios es el de irrenunciabilidad, este para Palavecino (2020) impide que los trabajadores renuncien a los derechos que la ley les otorga, aun por voluntad propia. Este responde a la naturaleza de orden público de la materia laboral y busca evitar que, por presión o necesidad, los empleados acepten condiciones que los perjudiquen o firmen cláusulas que los priven de sus beneficios legales para proteger la estabilidad social, el bienestar colectivo y asegurar que los derechos laborales sean efectivos. En Ecuador, este principio está consagrado en el artículo 4 del Código de Trabajo (2005) y en el artículo 326 de la Constitución (2008) que declaran la irrenunciabilidad e intangibilidad de los derechos laborales.

Igualmente, se debe mencionar el principio de continuidad de la relación laboral, como señala Rosenbaum (2023), busca proteger el trabajo como un bien jurídico, asegura que las

normas laborales reconozcan y respalden la permanencia y estabilidad del vínculo entre trabajador y empleador. Este se orienta a evitar despidos arbitrarios y a garantizar que el empleo sea una fuente segura de subsistencia y desarrollo para el empleado y su familia. Este se basa en que el empleado debe conservar su empleo hasta cumplir los requisitos legales para la jubilación o pensión, salvo causas justificadas de terminación. Asimismo, es fundamental para la estabilidad laboral, la protección social y la mejora de la calidad de vida del trabajador y su entorno.

Asimismo, hay que mencionar el principio de primacía de la realidad que se basa en que, ante discrepancias entre lo que se pacta formalmente en documentos y lo que ocurre en la práctica diaria del trabajo, deben prevalecer los hechos reales y concretos sobre lo escrito. Según Palavecino (2020) responde a la necesidad de reconocer la verdadera naturaleza del vínculo laboral, priorizando la situación objetiva del trabajador frente a posibles distorsiones contractuales. Su función es evitar que el empleador manipule o desvirtúe la relación laboral en perjuicio del trabajador. Esta salvaguarda al trabajador, especialmente dada su posición vulnerable, asegurando que la realidad del vínculo laboral sea la que determine los derechos y obligaciones de las partes.

Por último, está el principio de buena fe, que para Campos et al. (2022), constituye un estándar de conducta jurídica que exige a todas las personas actuar con rectitud, lealtad y honradez en sus relaciones y contratos al igual que se basa en la integridad y la corrección en cada actuación. Este implica obrar de manera clara y honesta, esperando que la otra parte actúe del mismo modo, y se sustenta en la intención y la confianza mutua.

Principios que rigen el tratamiento de datos personales

El artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPD) (2011) reconoce un grupo de principios que se aplican a la información personal entre ellos están, el principio de juridicidad referido a que el tratamiento de datos personales debe realizarse bajo el marco de la Constitución, los tratados internacionales ratificados, la propia ley, su reglamento y demás normativa aplicable. Ninguna acción sobre los datos puede contradecir los derechos y obligaciones fundamentales, y todo tratamiento debe poder ser justificado legalmente, para asegurar la protección de las personas ante cualquier uso indebido de su información.

Por otra parte, se regula en la Ley (2011) el principio de lealtad que exige que los datos personales sean tratados de manera honesta y clara, de modo que los titulares sepan en todo momento qué información se recoge, cómo se usa y con qué propósito. Se prohíbe el tratamiento de datos por medios engañosos, ilícitos o para fines desleales, asegurando que el titular nunca sea sorprendido o perjudicado por el uso de su información. Igualmente prevé el de transparencia que implica que toda información relacionada con el tratamiento de datos personales debe ser accesible y comprensible para el titular. Esto obliga a los responsables a utilizar un lenguaje sencillo y claro, y a mantener canales de comunicación abiertos para que los titulares puedan

informarse sobre cómo y por qué se usan sus datos. Así, se fomenta la confianza y se facilita el ejercicio de los derechos de los titulares.

Otro de los principios previstos en la norma objeto de examen (2021) es el de finalidad que se refiere a que, los datos personales, solo pueden ser tratados para fines determinados, explícitos y legítimos, los cuales deben ser comunicados previamente al titular. No está permitido cambiar la finalidad original sin una justificación legal o sin cumplir los requisitos para un nuevo tratamiento. Asimismo, se regula el principio de pertinencia y minimización que se basa en recolectar la cantidad de datos estrictamente necesaria para cumplir la finalidad declarada. No es válido solicitar o conservar información irrelevante o excesiva, lo que protege al titular de un uso desproporcionado de su información personal.

Por otra parte, la LOPDP (2021) establece el principio de proporcionalidad que se enfoca en que, el tratamiento de datos debe ser adecuado, relevante y no excesivo respecto a la finalidad perseguida. Esto implica que cada dato tratado debe tener una justificación clara y que no se pueden realizar tratamientos innecesarios o invasivos. También, preceptúa el principio de confidencialidad que exige que los datos personales se manejen con sigilo y secreto, y que no se divulguen ni utilicen para fines distintos a los autorizados. Los responsables deben implementar medidas organizativas y técnicas para garantizar que la información esté protegida frente a accesos no autorizados o filtraciones.

Del mismo modo, la normativa revisada (2021) reconoce entre los principios el de calidad y exactitud que se refiere a que, los datos personales deben ser precisos, completos, actualizados y comprobables. Si se detecta un error o inexactitud, el responsable tiene la obligación de corregirlo de inmediato. Igualmente regula el de conservación que se sustenta en que, los datos personales solo pueden ser almacenados durante el tiempo necesario para cumplir la finalidad para la que fueron recogidos. Una vez cumplido ese objetivo, deben ser eliminados, anonimizados o disociados, salvo que exista una razón legítima para su conservación.

El principio de seguridad es otro de los contemplados en la LOPDP (2021) cuyo básicamente es que se deben implementar todas las medidas técnicas y organizativas necesarias para proteger los datos personales frente a riesgos, amenazas o vulnerabilidades. Estas deben adaptarse al tipo de datos, su sensibilidad y el contexto en que se tratan, y deben ser revisadas y actualizadas periódicamente. Asimismo, el de responsabilidad proactiva y demostrada implica que el responsable del tratamiento debe ser capaz de demostrar en todo momento que cumple con los principios y obligaciones de la ley. Esto implica documentar procesos, aplicar buenas prácticas, certificaciones y rendir cuentas tanto ante los titulares como ante la autoridad de control.

Por último, la norma prevé el principio de aplicación favorable al titular y el de independencia del control. El primero, basado en que, en caso de duda sobre la interpretación de la ley o de los contratos, siempre deberá aplicarse la opción más favorable para el titular de los datos personales, priorizando la protección de sus derechos. El segundo se refiere a que, la

autoridad encargada de la protección de datos personales debe ejercer sus funciones de manera autónoma, imparcial e independiente, garantizando la vigilancia, prevención, investigación y sanción de cualquier incumplimiento de las normas.

Como se aprecia, la Ley Orgánica de Protección de Datos Personales integra varios principios que permiten interpretar y orientar la tutela de la información personal, mediante parámetros como la juridicidad, lealtad, transparencia, finalidad, proporcionalidad, entre otros antes desarrollados. Este marco normativo respeta los derechos fundamentales de las personas titulares de datos, exige su cumplimiento y la aplicación de prácticas adecuadas para que los datos sean debidamente salvaguardados por parte de los responsables.

Derecho al trabajo y a una vida digna

El derecho al trabajo es un derecho humano y como tal está consagrado en instrumentos internacionales como en la norma constitucional ecuatoriana (2008) en el artículo 33 como un derecho y a su vez un deber social de naturaleza social y un derecho de tipo económico. Por ello, el Estado debe asegurar a los empleados el pleno respeto a su dignidad, al igual que la remuneración correspondiente. Este debe ser elegido o aceptado de manera libre.

En ese sentido, Pérez (2017) considera que el derecho al trabajo implica una protección a la dignidad humana. Esto a partir de que es una fuente de ingresos, que coadyuva al desarrollo personal al igual que social permite crear relaciones y es la base del sustento individual y familia. Sin su ejercicio, como explica Monereo (2020), no es posible efectivizar otros derechos fundamentales como a la alimentación, la vivienda, salud, educación y otros.

En este contexto, el derecho al trabajo implica la posibilidad de acceder a un empleo digno, sin discriminación y bajo condiciones justas. El Comité de Derechos Económicos, Sociales y Culturales (2006) indica que el derecho al trabajo se concreta en la libertad de elegir empleo, la protección contra el trabajo forzado y el acceso a sistemas de protección social que aseguren el ejercicio efectivo de este derecho. Así, el derecho al trabajo protege la posibilidad de desempeñar ciertas funciones y exige condiciones laborales adecuadas y dignas.

Asimismo, el contenido del derecho al trabajo, según determina el Comité de Derechos Económicos, Sociales y Culturales en la Observación General N° 18 (2006) comprende tres componentes: la disponibilidad, la accesibilidad y la aceptabilidad y calidad. La primera, implica que los Estados deben promover servicios y políticas que faciliten el acceso a oportunidades laborales. La accesibilidad exige la eliminación de cualquier forma de discriminación y la promoción de la igualdad de oportunidades, incluyendo la adaptación de entornos laborales para personas con discapacidad. La aceptabilidad y calidad garantizan que los empleos sean seguros, justos y respetuosos de la dignidad humana.

Por su lado, la dignidad humana es para González (2017) un principio y un derecho. Esto se debe a que, como principio del ordenamiento jurídico su propósito, es guiar la correcta implementación de las normativas y prevenir cualquier conducta que la afecte. Además, tal como

indica Lara (2016) representa una regla de comportamiento y un límite para aplicar el derecho, por esto los derechos fundamentales deben garantizarla, en especial, el derecho al trabajo.

En el contexto de estudio, la inadecuada protección de los datos biométricos puede menoscabar el ejercicio pleno del derecho al trabajo y la dignidad humana, ya que contiene características únicas de las personas como las huellas dactilares, iris o rasgos faciales, lo que puede traer riesgos en cuanto a su identificación, rastreo y suplantación de identidad. Según Garriga (2024) cuando no se controlan estos datos, las consecuencias son irreversibles, ya que, los datos biométricos no pueden ser cambiados si se ven comprometidos. Esto puede generar discriminación, estigmatización y vulneración de la autonomía personal, ya que el individuo pierde el control sobre información íntima y que define su identidad.

Además, la exposición inadecuada de estos datos en contextos como el laboral, puede afectar la dignidad, el derecho a la intimidad y puede llegar a lesionar la reputación de una persona. Esto puede facilitar que se hagan perfiles sobre ella, que contemplen, intereses, relaciones, emociones, lo que puede usarse para influir o manipular decisiones personales sin que la persona lo sepa o lo consienta. La digitalización y almacenamiento de datos biométricos de los empleados como expone Muñoz (2022) se convierte en un registro informático en un dato que gestiona el centro laboral, lo que acrecienta el riesgo de que esta información sea utilizada para fines distintos a los inicialmente consentidos por el trabajador. Esto puede generar vulnerabilidades permanentes, si los datos biométricos son almacenados sin garantías adecuadas de seguridad y confidencialidad, por lo que, su salvaguarda efectiva es primordial.

RESULTADOS Y DISCUSIÓN

A partir del estudio desarrollado acerca del tratamiento de datos biométricos en el ámbito laboral ecuatoriano se manifiesta una tendencia enfocada a la incorporación de tecnologías biométricas en la gestión de recursos humanos, para lograr mayor seguridad y eficiencia a los procesos de identificación y control de acceso de los trabajadores a sus puestos laborales. Al respecto, el desarrollo de la tecnología ha llevado a pasar de métodos manuales de identificación a sistemas automatizados, lo que ha generado la aplicación de la biometría en entornos laborales. Sin embargo, este avance ha estado dado lugar a problemáticas éticas y jurídicos, en particular, en lo que concierne al consentimiento y la protección de los derechos fundamentales de los trabajadores.

Igualmente, del examen de la doctrina y la normativa se destaca la clasificación que se realiza de los datos biométricos como información sensible, lo que exige un tratamiento especial y la aplicación de garantías de protección. En el país, la Ley Orgánica de Protección de Datos Personales y su Reglamento establecen requisitos para el tratamiento de estos datos, como el consentimiento, informado del titular. Sin embargo, en la práctica, la obtención del consentimiento es deficiente, porque los trabajadores no reciben información suficiente, ni

comprensible sobre el uso de sus datos, lo que genera una distancia entre la normativa y su aplicación real.

Asimismo, se manifiesta una tensión entre el consentimiento otorgado por el trabajador y la salvaguarda de sus derechos, a partir de que el problema fundamental se manifiesta en que, aunque la LOPDP exige el consentimiento informado, libre y específico para el tratamiento de datos biométricos, que se consideran datos sensibles, en la práctica laboral ecuatoriana las condiciones de subordinación y dependencia pueden restringir la libertad del trabajador para rechazar o negociar dicho consentimiento. Ello representa un desequilibrio ya que, el consentimiento puede no cumplir con los criterios de voluntariedad exigidos por la ley, específicamente ante la relación desigual existente entre empleador y trabajador. Por ello es una dificultad, confiar solamente en el consentimiento como base legitimadora para el uso de datos biométricos en el ámbito laboral. Esto conlleva a que se estudien, apliquen e impongan más garantías y mecanismos de supervisión para proteger los derechos fundamentales y la autonomía de los trabajadores.

Por otro lado, la relación laboral presenta un desequilibrio de poder, lo que puede afectar la validez del consentimiento, pues el trabajador podría sentirse presionado a aceptar el tratamiento de sus datos biométricos para mantener su trabajo. Esto contradice la voluntariedad y la libertad del consentimiento, y plantea la necesidad de implementar mecanismos de protección para evitar abusos y garantizar la autonomía del trabajador.

En cuanto a los principios que rigen el tratamiento de datos biométricos, la doctrina concuerda en la importancia de la legalidad, proporcionalidad, transparencia y confidencialidad. No obstante, se identifican contradicciones en la interpretación y aplicación de estos principios, ya que la normativa exige que el tratamiento sea proporcional y limitado a lo necesario, en la práctica, muchas empresas, como exponen Borbor y Chaca (2024) recolectan y almacenan más datos de los requeridos, lo que puede afectar la privacidad y la dignidad de los trabajadores.

Asimismo, de la investigación realizada se evidencia que existen pocos estudios que analicen desde la práctica, el impacto de la biometría en el entorno laboral, la mayoría de los trabajos examinados tienen un enfoque doctrinal o normativo, lo que limita la identificación clara de los efectos que enfrentan los trabajadores en su cotidianidad. Esto reconoce la necesidad de estudiar mediante encuestas, entrevistas y estudios de caso la percepción de los empleados y la efectividad de los mecanismos de protección implementados.

Un aspecto que la revisión bibliográfica realizada evidencia es la suficiencia de las medidas de seguridad adoptadas por las empresas para proteger los datos biométricos, se reconocen avances en la implementación de tecnologías seguras y protocolos de acceso restringido, sin embargo, existe poca capacitación y concienciación en materia de protección de datos lo que conduce a sus filtraciones, usos indebidos y accesos no autorizados. Esta contradicción demuestra la necesidad de salvaguardar la privacidad y los datos personales.

Asimismo, el estudio llevado a cabo muestra coincidencia en cuanto a la importancia de respetar el derecho a la intimidad y la dignidad humana en el tratamiento de datos biométricos, tal como lo establecen instrumentos internacionales y la Constitución ecuatoriana. Por ello, desde una perspectiva legal, es primordial plantear que para proteger los referidos derechos, se obliga a los empleadores y al Estado a implementar salvaguardias efectivas que limiten el acceso y uso de datos biométricos laborales con fines legítimos y proporcionadas. Su empleo indebido, la discriminación o la exposición de la identidad de los trabajadores conducen a la transgresión de estos derechos fundamentales, lo que genera responsabilidad administrativa y constitucional. La digitalización y almacenamiento masivo de datos biométricos puede afectar la identidad de los trabajadores y exponerlos a riesgos permanentes, como la discriminación o el perfilado indebido. Por ello, se exige una protección adecuada y un mayor control.

Finalmente, lo antes expuesto en la discusión evidencia que, existe un marco normativo internacional y nacional que protege los datos personales y biométricos, aun cuando existen dificultades para aplicarlos en el ámbito laboral. Esto muestra contradicciones entre la teoría y la práctica, desconocimiento sobre los derechos y obligaciones y la ausencia de mecanismos de control y sanción ante la afectación al derecho a la protección de datos biométricos en el ámbito laboral.

CONCLUSIONES

En el estudio desarrollado, se constató que el empleo de tecnologías biométricas en el ámbito laboral ecuatoriano existe problemas que afectan la protección de los derechos fundamentales de los trabajadores, particularmente en lo referente a la privacidad, la intimidad y la dignidad personal. El análisis jurídico realizado demuestra que, aun cuando existe un marco normativo amplio, la Ley Orgánica de Protección de Datos Personales como en su Reglamento, existe una incongruencia entre la legislación y su aplicación efectiva, lo que se evidencia en la obtención deficiente o poco informada del consentimiento para el tratamiento de datos sensibles.

Además, el estudio expone que la posición de subordinación del trabajador frente al empleador afecta la autenticidad del consentimiento prestado, lo que puede generar una vulneración a los principios de voluntariedad, proporcionalidad y minimización exigidos por la ley. Desde el punto de vista jurídico, esto exige un control de la validez del consentimiento en el entorno laboral, a partir del desequilibrio existente entre la relación de poder entre empleador y empleado, lo que imponiendo a los primeros, el deber de adoptar salvaguardias adicionales, tales como información reforzada, garantías de no discriminación y canales para el ejercicio de derechos y reclamaciones.

Se concluye que, para que la protección de datos biométricos tenga un efecto protector en el ámbito laboral, no es suficiente con observar formalismos normativos, se deben aplicar prácticas empresariales sean sometidas a control y supervisión al igual que la imposición de

sanciones disuasorias ante vulneraciones comprobadas. Asimismo, los empleadores deben documentar y justificar la necesidad y proporcionalidad de la recolección de datos biométricos respecto a los fines perseguidos, evitando la automatización indiscriminada y el acopio masivo de información. Las autoridades, deben diseñar políticas y programas de capacitación y divulgación que permitan a los trabajadores comprender el alcance de sus derechos y actuar oportunamente ante eventuales abusos.

De esta forma, este estudio jurídico evidencia que la protección de datos biométricos laborales en Ecuador depende de la existencia de la normativa de la materia y de la interpretación y aplicación de los principios de voluntariedad, proporcionalidad y finalidad en las relaciones laborales. La falta de consentimiento libre, informado y real, agravada por el desequilibrio de poder entre las partes, puede transformar las prácticas biométricas en vulneraciones a la intimidad y la dignidad de los trabajadores, originando responsabilidad jurídica y obligando a los empleadores y autoridades a aplicar mecanismos de supervisión, rendición de cuentas y reparación. Por tanto, el cumplimiento normativo debe ser entendido como una obligación jurídica y no una simple formalidad, destinada a proteger los derechos fundamentales en el nuevo contexto tecnológico del entorno laboral ecuatoriano.

REFERENCIAS

- Aguirre, Á. (2023). *Uso de datos biométricos (biometría) como método para aceptar las políticas de uso de datos personales*. Retrieved 6 de julio de 2025, from backspace.uhemisferios.edu.ec:
<https://backspace.uhemisferios.edu.ec/server/api/core/bitstreams/40c840d4-958d-4d40-a9e8-41b57426b523/content>
- Alonso, M., y Casas, M. E. (2017). *Derecho del trabajo. Segunda edición*. Madrid, España: Civitas Ediciones, S. L.
- Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial No 449 de 20 de octubre de 2008.
- Asamblea General de la Organización de Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. ONU.
- Asamblea General de la Organización de Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos*. ONU.
- Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales (LOPD)*, . Registro Oficial Suplemento 459 de 26-may.-2021.
- Borbor, L., y Chaca, W. (2024). *Consentimiento en el uso de datos sensibles y la Ley Orgánica de Protección de Datos Personales en el ámbito privado*. Retrieved 6 de julio de 2025, from repositorio.upse.edu.ec: <https://repositorio.upse.edu.ec/handle/46000/12112>
- Campos, S., Munita, R., y Pereira, E. (2022). Fundamentación normativa de los deberes derivados de la buena fe contractual. Entre el individualismo desinteresado y el altruismo moderado. *Revista de Derecho Privado*, II(43), 187-217.
<https://doi.org/https://doi.org/10.18601/01234366.n43.08>
- Comité de Derechos Económicos, Sociales y Culturales. (2006). *Observación general N° 18*. Ginebra: DESC.
- Conferencia Especializada Interamericana sobre Derechos Humanos . (1969). *Convención Interamericana de Derechos Humanos*. OEA.
- Congreso Nacional. (2005). *Código de Trabajo*. Quito, Ecuador: Registro Oficial Suplemento 167 de 16-dic.-2005.
- Dworkin, R. (2014). *Filosofía del derecho*. México D.F: Fondo de Cultura Económica.
- Escajedo, L. (2017). *Tecnologías biométricas, identidad y derechos fundamentales*. Aranzadi.
- Garriga, A. (2024). Los derechos ante los sistemas biométricos que incorporan inteligencia artificial. *Derechos y Libertades*, 51(2), 117-149.
<https://doi.org/https://doi.org/10.20318/dyl.2024.8585>
- González, J. (2017). *La dignidad de la persona*. Curitiba: Juruá.
- Jain, K., Ross, A., y Prabhakar, S. (2017). *Una introducción al reconocimiento biométrico*. IEE.

- Lara, M. E. (21 de octubre de 2016). *www.derechoecuador.com*. Retrieved 6 de julio de 2025, from *www.derechoecuador.com*: <https://www.derechoecuador.com/la-dignidad-humana-y-el-derecho-a-la-vida-frente-al-cambio-climatico>
- Mercader, J. (2020). *Datos biométricos en los centros de trabajo*. Wolters Kluwer.
- Mercader, J. (2023). El “big bang” de la biometría laboral. e la huella dactilar a los neurodatos. *Labos*, 5(2), 4-23. <https://doi.org/10.20318/labos.2024.8749>
- Monereo, J. L. (2020). *Manual de derecho del trabajo*. Comares.
- Muñoz, A. B. (2022). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Tirant Lo Blanch.
- Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (1988). *Observación General No 16 sobre el derecho a la intimidad*. ONU.
- Palavecino, C. (2020). *Los principios del Derecho del Trabajo*. Retrieved 14 de febrero de 2025, from *www.u-cursos.cl*: https://www.u-cursos.cl/derecho/2012/2/D128A0523/2/material_docente/bajar?id=657849
- Pérez, A. (2017). *Derechos humanos. Estado de derecho y constitución 2da Edición*. Madrid: Tecnos.
- Plá, A. (2016). *Los principios del derecho del trabajo. Cuarta edición*. Montevideo, Uruguay: Fundación de Cultura Universitaria.
- Presidencia de la República del Ecuador. (2023). *Reglamento General de la Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 435 del 13 de noviembre de 2023.
- Rodriguez, M. (2019). Las facultades de control de datos biométricos del trabajador. *Temas laborales*, 4(150), 91-109. Retrieved 7 de julio de 2025, from <http://Dialnet-LasFacultadesDeControlDeDatosBiometricosDelTrabaja-7224369.pdf>
- Rosenbaum, F. (2023). Debate: Actualidad y vigencia de los principios del Derecho del Trabajo. *Revista Jurídica del Trabajo*, 4(10), 130–135. Retrieved 8 de julio de 2025, from <http://revistajuridicadeltrabajo.com/index.php/rjt/article/view/160>
- Ruiz, M., Rodríguez, J., y Olivares, J. C. (2009). Una mirada a la biometría. *Revista Avances en Sistemas e Informática*, 6(2), 29-38. Retrieved 6 de julio de 2025, from <https://www.redalyc.org/pdf/1331/133113598005.pdf>
- Villa, W., Cadena, J., Gavilanez, ', y Centeno, C. (2024). Protección de Datos Personales en Ecuador y Colombia: Principios, Ética y Desafíos Actuales. *Revista Científica de Informática ENCRYPTAR*, 6(11), 19-34. <https://doi.org/https://doi.org/10.56124/encryptar.v6i11.0002>