

**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**

**Facultad de Derecho**



**Programa de Segunda Especialidad en Derecho del Trabajo y  
de la Seguridad Social**

*“Ius variandi digital: alcances y límites al poder de dirección del  
empleador en el marco de la inteligencia artificial en el Perú”*

Trabajo académico para optar el título de Segunda Especialidad en  
Derecho del Trabajo y de la Seguridad Social

Autora:

***Astrid Maricela Bárraga Ochoa***

Asesor:

***Willman Cesar Melendez Trigos***

Lima, 2025

## Informe de Similitud


Yo, MELENDEZ TRIGOSO, WILLMAN CESAR, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo Académico titulado “Ius variandi digital: alcances y límites al poder de dirección del empleador en el marco de la inteligencia artificial en el Perú”, del autor(a) BARRAGA OCHOA, ASTRID MARICELA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 31%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 07/12/2025.

- He revisado con detalle dicho reporte y el Trabajo Académico, y no se advierten indicios de plagio.

- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, 12 de diciembre del 2025

MELENDEZ TRIGOSO, WILLMAN CESAR	
DNI: 42821994	
ORCID: <a href="https://orcid.org/0000-0002-3782-4332">https://orcid.org/0000-0002-3782-4332</a>	

## RESUMEN

El presente trabajo de investigación tiene por finalidad analizar el ejercicio del poder de dirección en la era de la transformación digital, en especial a partir del uso de tecnologías como la videovigilancia, el control biométrico y los algoritmos en el marco de la gestión laboral. Este nuevo panorama exige que nuestro ordenamiento jurídico contemple una regulación acorde a los nuevos cambios estructurales y tecnológicos, así como límite cualquier tipo de uso que vulnere derechos fundamentales —como la intimidad, la dignidad y la protección de datos personales—, así como los estándares internacionales dentro del marco de la relación de trabajo.

De esta manera, la presente investigación tiene por objetivo demostrar que la implementación de dispositivos tecnológicos —tales como sistemas automatizados y la incorporación de la inteligencia artificial en la gestión laboral — utilizados por los empleadores para supervisar, evaluar o controlar el desempeño de los trabajadores deben ajustarse a los principios de razonabilidad, proporcionalidad, finalidad legítima y respeto por los derechos fundamentales de los trabajadores. Con ello se busca evitar que el poder de dirección se transforme en un mecanismo de vigilancia invasiva y/o discriminatoria.

Finalmente, las conclusiones a las que llega la presente investigación es que el creciente avance tecnológico impone al derecho laboral el desafío de redefinir los alcances del *ius variandi* en una era digital, así como de establecer un equilibrio entre desarrollo tecnológico de las empresas y la tutela de los trabajadores.

### Palabras clave

Ius Variandi — Protección de datos personales — Inteligencia Artificial — Poder de dirección — Videovigilancia — Derecho a la intimidad

## **ABSTRACT**

The present research aims to analyze the exercise of managerial authority (poder de dirección) in the era of digital transformation, particularly regarding the use of technologies such as video surveillance, biometric control, and algorithmic systems within labor management. This new scenario demands that the Peruvian legal framework adapt to current structural and technological changes, setting clear limits to prevent any use that may infringe upon fundamental rights—such as privacy, dignity, and the protection of personal data—as well as ensuring compliance with international labor standards.

Accordingly, this study seeks to demonstrate that the implementation of technological devices—such as automated systems and the incorporation of artificial intelligence in labor management—used by employers to supervise, evaluate, or monitor workers' performance must comply with the principles of reasonableness, proportionality, legitimate purpose, and respect for fundamental labor rights. This is essential to prevent managerial authority from becoming a mechanism of invasive and/or discriminatory surveillance.

Finally, the research concludes that rapid technological advancement poses a significant challenge for labor law: redefining the scope of *ius variandi* in the digital era and achieving a balance between corporate technological development and the protection of workers' rights.

### **Keywords**

Ius Variandi — Personal Data Protection — Artificial Intelligence — Managerial Authority — Video Surveillance — Right to Privacy.

## ÍNDICE

<b>I. INTRODUCCIÓN .....</b>	<b>4</b>
<b>II. EL PODER DE DIRECCIÓN EN LA ERA DIGITAL .....</b>	<b>6</b>
<b>II.1. EL <i>IUS VARIANDI</i> CLÁSICO Y EL <i>IUS VARIANDI</i> DIGITAL .....</b>	<b>9</b>
<b>III. EL USO DE TECNOLOGÍAS DE CONTROL EN EL TRABAJO Y SUS IMPLICANCIAS JURÍDICAS .....</b>	<b>12</b>
<b>III.1. VIDEOVIGILANCIA EN CENTROS LABORALES .....</b>	<b>15</b>
<b>III.2. TRATAMIENTO DE DATOS BIOMÉTRICOS .....</b>	<b>18</b>
<b>IV. NORMATIVA PERUANA QUE REGULA Y PROMUEVE EL USO DE LA INTELIGENCIA ARTIFICIAL .....</b>	<b>23</b>
<b>IV.1. PRINCIPIOS RECTORES DE LA INTELIGENCIA ARTIFICIAL     APLICADOS AL ÁMBITO LABORAL .....</b>	<b>24</b>
<b>IV.2. RIESGOS LABORALES DERIVADOS DEL USO DE INTELIGENCIA     ARTIFICIAL .....</b>	<b>28</b>
<b>V. PROTECCIÓN DE LOS DERECHOS LABORALES EN EL ENTORNO DIGITAL .....</b>	<b>31</b>
<b>VI. CONCLUSIONES.....</b>	<b>34</b>
<b>BIBLIOGRAFÍA.....</b>	<b>36</b>

## I. INTRODUCCIÓN

Las tecnologías de la información y la comunicación (TIC) han transformado el mundo laboral, ampliando el poder de dirección y control por parte del empleador. De forma particular, podemos observar cómo en el artículo 9 del Texto Único Ordenado del Decreto Legislativo N.º 728, se reconoce que el poder de dirección del empleador habilita ciertas modificaciones organizativas — incluido el uso de medios tecnológicos— siempre que se respeten la razonabilidad, proporcionalidad y la dignidad de la persona trabajadora. No obstante, en la práctica los límites del control empresarial cuando se implementan herramientas digitales como la videovigilancia algorítmica, biometría y toma de decisiones automatizadas en el lugar de trabajo aún son ambiguos y poco delimitados. Esta situación genera diversas dudas de cómo aplicar el poder de dirección en la era digital sin vulnerar los derechos de los trabajadores.

Asimismo, la incorporación de la inteligencia artificial (IA) ha potenciado este fenómeno, lo que está generando enormes desafíos legales con respecto a la automatización y el manejo algorítmico en las relaciones laborales. En otras palabras, el uso de herramientas digitales y sistemas inteligentes ha afectado significativamente los derechos fundamentales de los trabajadores, especialmente su derecho a la privacidad, que se está viendo cada vez más invadido.

Lo anterior evidencia múltiples problemas sobre cómo se ejerce el *ius variandi* en entornos digitales. Por ejemplo, la gestión algorítmica plantea en entornos laborales sus propios retos como la toma de decisiones automatizadas que podrían convertirse en decisiones subjetivas o caracterizadas por sesgos, como ocurre en las evaluaciones, asignaciones, sanciones o selección de personal que se realiza con el uso de inteligencia artificial.

Estos sesgos pueden producirse por la calidad de los datos o por su diseño, así como por la falta supervisión humana efectiva y vías reales de impugnación. Por otro lado, el tratamiento de datos biométricos, por ser sensibles, muchas veces no cuenta con bases de licitud sólidas ni con consentimiento informado suficiente; ello genera que persisten asimetrías de información que impiden al trabajador comprender y cuestionar el sistema. Finalmente, en el plano institucional, en el caso peruano el marco regulador existente para la IA en el ámbito laboral sigue siendo insuficiente para abordar las problemáticas anteriormente señaladas por su carácter general y poco operativo.

También se observan varias carencias, como la coordinación deficiente entre las entidades de protección de datos personales y las Autoridades Administrativas del Trabajo (SUNAFIL), la poca jurisprudencia en cuanto a videovigilancia algorítmica y la escasa participación sindical en el uso de tecnologías en los lugares de trabajo. Estas deficiencias obstaculizan la creación de un modelo equilibrado de gobernanza tecnológica, que sea capaz de conciliar la innovación y la productividad de las empresas con una supervisión sólida y efectiva de los derechos de los empleados.

En vista de ello, el presente trabajo está conformado por tres capítulos que abordan los problemas planteados. El primer capítulo se centra en el poder de dirección empresarial en la era digital, el cual ha variado en el tiempo, pues se redefine desde el *ius variandi* clásico y se formula una noción operativa de *ius variandi* digital, a partir de las manifestaciones que se configuran en los nuevos entornos de trabajo como los horarios de conexión, software de supervisión, métricas algorítmicas. Asimismo, se analiza de manera transversal los límites como la razonabilidad, proporcionalidad, respeto a derechos fundamentales, privacidad, desconexión digital y protección de datos.

En el segundo capítulo, se analizará el uso de tecnologías de control en el trabajo y sus implicancias jurídicas, entre los cuales figuran i) la videovigilancia en centros laborales y ii) el tratamiento de datos biométricos en el registro de

jornada laboral. Asimismo, se analizará su impacto y sus riesgos a raíz de la reciente Ley N.º 31814, Ley que Promueve el Uso de la Inteligencia Artificial en Favor del Desarrollo Económico y Social del País, y su Reglamento regulado mediante el Decreto Supremo N.º 115-2025-PCM.

En el tercer capítulo, se abordará la protección de los derechos laborales en el entorno digital, examinando si la regulación interna peruana se ajusta —por finalidad legítima, necesidad, idoneidad y menor lesividad— a los estándares internacionales de la Organización Internacional del Trabajo y a referentes internacionales comparados como el Reglamento General de Protección de Datos de la Unión Europea y el Reglamento de Inteligencia Artificial de la Unión Europea (“AI Act”).

Finalmente, se realizará un análisis crítico de la normativa peruana vinculada a la inteligencia artificial en el ámbito laboral y se planteará una propuesta de mejora en cuanto a la gobernanza tecnológica garantista con transparencia algorítmica, participación sindical, auditorías y canales eficaces de reclamación, a fin de equilibrar innovación, productividad y tutela reforzada de los trabajadores.

## **II. EL PODER DE DIRECCIÓN EN LA ERA DIGITAL**

En los últimos años, los progresos tecnológicos han impactado significativamente en la sociedad, propiciando una mayor interconexión y digitalización. En este contexto, la transformación digital también ha impactado en aspectos importantes de nuestras vidas: el trabajo.

Desde la invención de tecnologías que automatizan los procesos de producción hasta la implementación de inteligencia artificial (IA) para administrar empresas, el empleo de nuevas tecnologías en el entorno laboral ha contribuido a optimizar las condiciones laborales y la productividad. De forma específica, en el presente

informe abordaremos el impacto de la IA y el poder dirección como parte del eje transversal a toda la relación laboral.

El derecho a la libertad de empresa, que está reconocido en el artículo 59 de la Constitución, es el fundamento constitucional del poder de dirección del empresario. Esta libertad abarca, entre otros aspectos, el derecho a organizarse, lo que permite al empresario organizar y gestionar su actividad económica de acuerdo con sus intereses.

Esto incluye establecer políticas de gestión de personal y contratación (Blancas, 2007, p. 105). En este contexto, el empleador tiene la capacidad de no solo dar órdenes e instrucciones, sino también de crear procedimientos para garantizar que se cumplan; esto es esencial para lograr los objetivos empresariales previstos.

Bajo esa óptica, la autoridad de gestión conferida al empleador se manifiesta en su habilidad para establecer normas laborales, impartir instrucciones indispensables para su realización y tomar medidas disciplinarias de manera razonable. Así, las facultades que surgen del poder de dirección del empleador están explícitamente establecidas en nuestro sistema legal, conforme al artículo 9 de la Ley de Productividad y Competitividad Laboral (en adelante, "LPCL"):

Artículo 9.- Por la subordinación, el trabajador presta sus servicios bajo dirección de su empleador, **el cual tiene facultades para normar reglamentariamente las labores, dictar las órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente,** dentro de los límites de la razonabilidad, cualquier infracción o incumplimiento de las obligaciones a cargo del trabajador. El empleador está facultado para introducir cambios o modificar turnos, días u horas de trabajo, así como la forma y modalidad de la prestación de las labores, **dentro de criterios de razonabilidad y teniendo en cuenta las necesidades del centro de trabajo.** (Énfasis añadido)

Además, es importante tener presente que la subordinación es *"el tercer y más complejo elemento esencial de la relación laboral"*, y significa que quien emplea tiene la capacidad de *"dirigir o conducir las actividades enmarcadas en una relación laboral"* (Vílchez Garcés, 2020, p. 649). Este poder directivo tiene su base en el derecho constitucional a la libertad de empresa, consagrado en el artículo 59 de la Constitución Política, que se define como un "derecho económico esencial que salvaguarda la autodeterminación individual para llevar a cabo actividades empresariales en sus múltiples formas" (Landa, 2017, citado por Vílchez Garcés, 2020, p. 649).

Según el Tribunal Constitucional (Exp. N.º 01405-2010-PA/TC), la libertad de empresa establece lo siguiente:

"De este modo, cuando el artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, está garantizando a todas las personas una libertad de decisión no sólo para crear empresas (libertad de fundación de una empresa), y por tanto, para actuar en el mercado (libertad de acceso al mercado), sino también para establecer **los propios objetivos de la empresa (libertad de organización del empresario) y dirigir y planificar su actividad (libertad de dirección de la empresa) en atención a sus recursos y a las condiciones del propio mercado, así como la libertad de cesación o de salida del mercado.** En buena cuenta, la Constitución a través del derecho a la libertad de empresa garantiza el inicio y el mantenimiento de la actividad empresarial en condiciones de libertad; así como la actuación, ejercicio o permanencia, en condiciones de igualdad, de la actividad empresarial y los agentes económicos en el mercado y la protección de la existencia de la empresa." (Énfasis añadido)

En esa misma línea, el empleador, en virtud de ese marco constitucional, está *"en la facultad de guiar el trabajo de sus empleados hacia los objetivos que ha establecido como propietario de la empresa"* (Toyama, 2020; citado en Vílchez

Garcés, 2020, p. 649). De esta manera, Landa, Toyama y Vílchez están de acuerdo en que el empleador tiene el derecho legítimo de organizar, supervisar y guiar las labores de sus trabajadores, tomando las decisiones necesarias para alcanzar los objetivos de la empresa. Este poder abarca la facultad de impartir instrucciones y de imponer sanciones disciplinarias, dentro del marco legal establecido y con respeto a los derechos fundamentales del trabajador.

Según la doctrina, las medidas adoptadas por el empleador no son absolutas, ya que las modificaciones y condiciones de trabajo deben cumplir con ser razonables y necesarias, por lo que la lesión de derechos fundamentales al trabajador constituye un límite válido (Ramos, 2019, p. 49).

Bajo ese panorama, la tecnología, ha permitido al empleador contar con herramientas que permitan fiscalizar, sancionar y dirigir la relación laboral a fin de poder evitar incumplimientos por parte de los trabajadores, mejorar la seguridad y garantizar el respeto y la disciplina laboral. No obstante, pese a sus beneficios, su uso inadecuado puede afectar derechos fundamentales de los trabajadores y limitar el poder de dirección del empleador.

## **II.1. EL *IUS VARIANDI* CLÁSICO Y EL *IUS VARIANDI* DIGITAL**

Ahora bien, para Boza (2020, p. 86), el empleador ejerce su autoridad a través de un conjunto de facultades para regular el trabajo de su personal. Por otro lado, dentro de las atribuciones que posee el empleador como titular del poder de dirección, se encuentran, principalmente, las siguientes (Vílchez Garcés, 2020, p. 649):

- Establecer los criterios de selección y reclutamiento al contratar personal nuevo y al promover ascensos o mejoras laborales.
- Planificar las tareas, determinando la manera en que se llevarán a cabo, la distribución de las actividades entre el personal y los procesos de producción, así como el sitio donde se llevarán a cabo dichas labores.

- Establecer directrices y normativas, tanto de forma oral como escrita, para regular las tareas, políticas internas, gestión de descripciones de puestos, fijación de horarios, jornadas y turnos laborales, entre otros aspectos.
- Velar por la correcta realización de las tareas por parte del equipo de trabajo.
- Sancionar los comportamientos que representen violaciones a los deberes laborales, a través de la implementación de acciones disciplinarias según la seriedad de las infracciones realizadas, como advertencias, suspensiones y despidos.

Por esa razón, con el paso del tiempo, las competencias del empleador y la extensión de su poder de dirección han cambiado gradualmente. En sus inicios, este poder se extendía sobre un modelo tradicional de organización del trabajo en persona, ejecutado dentro del centro de trabajo y bajo una supervisión directa. No obstante, el desarrollo de las tecnologías de la información y la comunicación ha modificado de manera significativa este modelo tradicional.

El control ya no se restringe hoy en día a la supervisión física de los empleados en las fábricas o las oficinas, sino que abarca también contextos virtuales donde el empleador tiene que supervisar y dirigir la prestación de servicios remotos usando dispositivos tecnológicos como sistemas de geolocalización, ordenadores o plataformas digitales.

Además, el impacto de la tecnología ha posibilitado la aparición de sistemas sofisticados de monitoreo, evaluación del rendimiento y decisiones automatizadas por medio de inteligencia artificial, lo que ha creado un escenario mucho más complejo que el que el derecho laboral había previsto originalmente.

Un ejemplo de ello es la digitalización de procesos, el teletrabajo y la gestión mediante inteligencia artificial han desplazado parte del control desde el espacio físico de la empresa hacia entornos virtuales y ubicuos, donde la coordinación, supervisión y evaluación del desempeño se apoyan en plataformas, registros

biométricos, analítica de datos y, cada vez más, en sistemas algorítmicos. Este tránsito exige reinterpretar las facultades directrices a la luz de los principios del derecho del trabajo, evitando que el desarrollo tecnológico se traduzca en injerencias desproporcionadas en la esfera personal del trabajador.

Otro ejemplo de ello es el uso de los medios informáticos y tecnológicos dentro del ámbito laboral, el empleador debe fiscalizar, sancionar y dirigir respetando los derechos del trabajador, informando los medios y fines, y eligiendo los mecanismos menos lesivos posibles a los derechos de los trabajadores (Toyama & Girado, 2014, p. 180). De esta forma, se observa como el *ius variandi* se ha acomodado progresivamente a los cambios tecnológicos: de un poder de dirección pensado para espacios comunes y horarios acotados (el centro de trabajo y la jornada) ha pasado a operar en entornos digitales ubicuos, donde la organización, supervisión y disciplina se ejecutan mediante plataformas, datos y algoritmos.

En esta nueva situación, el control no solo depende de que el trabajador esté presente físicamente en su lugar de trabajo, sino también de la digitalización del servicio. Es decir, se basa en la constante recopilación y análisis de datos que surgen directamente del desarrollo de la actividad (como registros de conexión, huellas dactilares, geolocalización y métricas de productividad, entre otros).

Esto contrasta con el modelo convencional de monitoreo laboral, que se llevaba a cabo en un espacio físico compartido y mediante supervisión directa y visible. No obstante, con la inclusión de cambios tecnológicos, que no existían antes, se optimiza la eficiencia en la organización del trabajo. Si bien parece un aspecto positivo, también incrementa el riesgo de vulnerar derechos inespecíficos de los trabajadores como su intimidad y privacidad, lo que permite replantear los límites del *ius variandi digital*.

Como lo hemos ido señalando, la irrupción de la inteligencia artificial acelera esta transición al habilitar formas de vigilancia algorítmica y toma de decisiones

automatizadas que pueden extenderse más allá del establecimiento y, en ocasiones, más allá de la jornada: monitoreo de actividad en dispositivos, análisis de patrones de productividad, asignación dinámica de tareas o detección de “anomalías” en tiempo real.

Ello desplaza el poder de fiscalización hacia esferas más próximas a la persona trabajadora (hogar, dispositivos personales, ritmos de vida), con el consiguiente riesgo de sobre injerencia y de afectación a la intimidad, la dignidad y el derecho a la desconexión.

Por eso, la adaptación del *ius variandi* al entorno digital no amplía ilimitadamente el control, sino que reformula sus condiciones de validez. Toda medida debe anclarse en causa objetiva, ser idónea, necesaria y la menos lesiva, respetar el núcleo esencial del contrato y las fronteras materiales y temporales del control (no vigilancia fuera de jornada, no intromisión en espacios sensibles o datos personales sensibles).

Por ello, cuando intervienen sistemas de IA, se añaden exigencias de transparencia, supervisión humana significativa, aplicabilidad, minimización y seguridad de datos, y —si hay datos sensibles, como biométricos— consentimiento expreso y salvaguardas reforzadas.

En síntesis, el *ius variandi* digital acompaña la transformación tecnológica, pero se subordina a un estándar garantista que equilibre eficiencia organizativa y tutela reforzada de los derechos fundamentales.

### **III. EL USO DE TECNOLOGÍAS DE CONTROL EN EL TRABAJO Y SUS IMPLICANCIAS JURÍDICAS**

La tecnología —y, en particular, la inteligencia artificial— ya se aplica en el ámbito laboral. En consecuencia, resulta imprescindible reconocer sus aportes a la gestión empresarial y, al mismo tiempo, evaluar de manera sistemática su

impacto y su incidencia en los derechos fundamentales de las personas trabajadoras involucradas en el despliegue de esta herramienta. Tomando ello en consideración, resulta prioritario analizar el impacto de las nuevas tecnologías en la gestión laboral, en particular su papel para reducir contingencias operativas, optimizar la asignación de tareas y mejorar la toma de decisiones.

De manera específica, se examinará cómo la inteligencia artificial, integrada con dispositivos tecnológicos, viene aplicándose en sectores importantes de nuestro país. En otros términos, la IA se perfila como un instrumento clave para fortalecer la gestión de personal. No obstante, antes de abordar casos de uso, delimitaremos conceptualmente: ¿qué es la IA?, ¿para qué sirve en la organización y gestión en el trabajo? ¿Cómo se aplica en el caso peruano? ¿De qué manera influye en los límites del poder dirección?

Como primera respuesta tenemos que la inteligencia artificial se define como *"un conjunto de tecnologías capaces de aprender, razonar y tomar decisiones, y su implementación en la seguridad y salud en el trabajo transforma radicalmente la prevención de riesgos, la vigilancia médica y la gestión operativa"* (Fajardo-López et al., 2023, p. 1). Ahora bien, en cuanto a su definición en el ámbito laboral, se caracteriza por *"la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano"* (Macías, 2022, p. 85).

Asimismo, la IA depende de la *big data* para generar información y su concepto se caracteriza por lo siguiente:

[...] hace referencia a dos cuestiones íntimamente relacionadas. En primer lugar, a la gran cantidad de datos disponibles, es decir a la existencia de un masivo volumen de datos que pueden ser utilizados con diversos fines y están al alcance de empresas, estados y particulares. En segundo lugar, con la expresión Big Data se alude también al **conjunto de tecnologías cuyo objetivo es tratar grandes cantidades de información, de datos, empleando complejos algoritmos y estadística** con la finalidad de hacer

predicciones, extraer información oculta o correlaciones imprevistas y, en último término, favorecer la toma de decisiones (Garriga, 2016, p. 28). (Énfasis agregado)

A efectos de enmarcar el análisis, conviene partir de un dato empírico y doctrinal: el uso de la inteligencia artificial en el trabajo “presenta tanto riesgos como desafíos” para las personas trabajadoras —automatización y posibles sesgos en selección, por un lado; exigencias de adaptación y garantías de decisiones justas, por otro—, lo que demanda medidas específicas de tutela (Torres Cadillo, 2023, p. 290). Lo que Torres Cadillo señala demuestra que la inteligencia artificial no solamente conlleva una transformación tecnológica, sino también la obligación de adecuar las regulaciones laborales y los sistemas de protección ante situaciones como el reemplazo automatizado de funciones, el surgimiento de prejuicios en las decisiones y la precariedad laboral.

Además, la cuarta revolución industrial ha agudizado el debate jurídico y ético debido a la pérdida de privacidad y al uso masivo de *big data*. Esto requiere una reconsideración del derecho laboral frente a tecnologías que fortalecen el poder de vigilancia de las empresas (Torres Cadillo, 2023, pp. 291–292). Se observa aquí un conflicto entre la eficacia de las empresas y los derechos esenciales, sobre todo el derecho a la privacidad y el derecho a decidir sobre la propia información. Así, el procesamiento a gran escala de datos personales a raíz de la relación laboral puede llevar a un control excesivo y poco transparente, por lo cual es esencial fortalecer principios como la proporcionalidad, el propósito y la mínima injerencia en el ámbito privado del empleado.

En el ámbito organizativo, los algoritmos y la inteligencia artificial ya afectan la gestión de personas —desde las decisiones sobre despidos y contrataciones hasta el control diario— y permiten supervisiones digitales a través de correo corporativo, videovigilancia, mensajería, navegación o geolocalización. Esto supone riesgos claros para la autodeterminación informativa y la privacidad si no se establecen límites en cuanto a finalidad, necesidad y transparencia (Torres Cadillo, 2023, pp. 292-293; 300; 306). El autor subraya que la supervisión tecnológica tiene el potencial de convertirse en una vigilancia continua y

desigual, lo cual puede tener un impacto negativo sobre la dignidad del empleado.

A continuación, se llevará a cabo un análisis de tres herramientas tecnológicas basadas en inteligencia artificial que se utilizan en la gestión laboral: (i) la videovigilancia algorítmica en los entornos laborales y (ii) el tratamiento de datos biométricos para el control de jornada y accesos.

### **III.1. VIDEOVIGILANCIA EN CENTROS LABORALES**

La vigilancia a través de video en el ámbito laboral, en particular cuando incorpora inteligencia artificial, implica un cambio significativo en la supervisión empresarial. La videovigilancia moderna no se limita a capturar imágenes, sino que *"detecta patrones y tendencias en la realidad observada (...) generando un riesgo real de discriminación algorítmica"* (Rodríguez-Piñero, 2024, p.77). Estos sistemas que clasifican perfilan y anticipan comportamientos, permiten al empleador tomar decisiones automatizadas que afectan de manera directa los derechos de trabajo (como evaluaciones, sanciones e incluso despidos). El peligro jurídico está en que los algoritmos utilizan información que puede tener prejuicios estructurales, replicando o acentuando discriminaciones ocultas en elementos como la conducta, la productividad y el rendimiento, lo cual requiere estándares aumentados de transparencia, control humano y no discriminación.

De igual manera, la autora enfatiza que *"la consciencia de estar continuamente monitorizado puede afectar negativamente a las personas, produciendo ansiedad y condicionando sus comportamientos"* (Rodríguez-Piñero, 2024, p. 76). Ello significa que la supervisión constante provoca un impacto de autocensura y estrés en el trabajo, lo que perjudica el desarrollo libre de la personalidad y deteriora el clima laboral.

Además, advierte que en la supervisión actual *"es la tecnología la que determina cómo se trabaja, y cómo se supervisa lo que se trabaja"* (Rodríguez-Piñero, 2024, p. 69). Este análisis muestra un proceso de automatización del poder

directivo, en el cual la supervisión deja de ser una conducta controlada por las personas y empieza a estar sujeta a lógicas algorítmicas que son difíciles de entender para el empleado. Ahora bien, que se tomen decisiones en base a sistemas poco transparentes impacta el principio de transparencia y pone en riesgo garantías fundamentales de toda relación laboral: el derecho a ser informado, a defenderse y a cuestionar el criterio de evaluación que se empleó

En relación con los riesgos jurídicos, se afirma que *“la videovigilancia inteligente se convierte en un control intrusivo, cuyo avance técnico incrementa los riesgos para los trabajadores”* (Rodríguez-Piñero, 2024, p. 82). Ello quiere decir que la supervisión se intensifica y se amplía en virtud del avance tecnológico, lo que facilita el registro, almacenamiento y análisis de datos relacionados con las interacciones interpersonales, los patrones de comportamiento, los períodos de descanso y los desplazamientos en el entorno laboral. Esto requiere la implementación de un criterio de proporcionalidad riguroso que considere la valoración de la idoneidad, la necesidad y la ponderación

Finalmente, la doctrina destaca que este tipo de control es invisible y automatizado, y por tanto requiere una regulación clara: *“la videovigilancia inteligente debe disponer de un marco regulatorio adecuado (...) evitando los riesgos para las personas que trabajan sometidas a ella”* (Rodríguez-Piñero, 2024, p. 82). De esta forma, la asimetría de poder inherente a la relación laboral se agrava con el hecho de que el trabajador no sabe cuándo, cómo ni hasta qué punto está siendo monitoreado. Por esta razón, el empleador tiene que comunicar de antemano la manera en que opera el sistema, los propósitos del procesamiento de datos y los procedimientos para impugnar decisiones automatizadas.

En el ámbito comparado, Rodríguez-Piñero señala que la difusión de sistemas sofisticados de videovigilancia inteligente en Europa requiere un fortalecimiento de la regulación para impedir que los derechos de los empleados sean vulnerados. En ese sentido, la autora precisa que *“la videovigilancia inteligente debe disponer de un marco regulatorio adecuado (...) evitando los riesgos para*

las personas que trabajan sometidas a ella” (Rodríguez-Piñero Royo, 2024, p. 82).

Desde este punto de comparación, es significativo realizar un análisis del estado presente de estas tecnologías en el Perú. Un ejemplo de ello es Fiberlux, una empresa que brinda servicios de videovigilancia en Perú mediante inteligencia artificial, a los que se les conoce como Video Surveillance as a Service (VSaaS).

Su sistema se centra en la identificación facial, el rastreo de objetos y el análisis del comportamiento en tiempo real son algunos de los servicios que se mencionan (Fiberlux, 2020). Asimismo, las cámaras que se utilizan tienen la habilidad de "identificar varios patrones de conducta para optimizar recursos y personal". Ello ayuda a integrar tecnologías de detección facial y aprendizaje automático en la infraestructura de seguridad. La puesta en marcha de sistemas que supervisen el cumplimiento de tareas, control de accesos o monitoreen los movimientos de los empleados en entornos laborales incluye retos legales significativos. Estos desafíos están vinculados con el principio de proporcionalidad y el derecho a la privacidad, ya que se está hablando del análisis algorítmico de imágenes, lo cual supone un tratamiento automatizado de datos biométricos personales. Siendo ello así, la implementación de sistemas de cámaras con tecnología de reconocimiento facial debe ser fundamentada en una necesidad estricta, ya que debe estar acompañada de información previa clara y que se someta a un proceso de revisión por parte de un ser humano, con el objetivo de prevenir posibles vulneraciones a la dignidad del trabajador.

Por su parte, Loratech, una compañía tecnológica, ha fomentado en Perú sistemas de vigilancia por video que utilizan inteligencia artificial y tienen la capacidad de "analizar y comprender lo que observan en tiempo real". Dichos sistemas combinan control de aforo, detección de conducta y reconocimiento facial en ambientes industriales y corporativos (Loratech, 2024). Por ello, las empresas privadas y las entidades públicas emplean estas plataformas, que operan a través de redes de cámaras vinculadas con software de análisis predictivo, para mejorar la seguridad organizacional y física.

### III.2. TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos son "*todas las características físicas, fisiológicas o conductuales de un individuo que posibilitan o validan su identificación única*" (Mercader Uguina, 2020, p. 2). Ejemplos de estos datos son: geometría de la mano, reconocimiento facial, constantes fisiológicas, huellas dactilares o patrones del iris, ya que este procesamiento implica características corporales inalterables, se trata de una información particularmente delicada, directamente relacionada con la dignidad y privacidad del empleado.

Por eso, el autor previene que la identidad biológica es individual para cada persona y, por ende, cualquier herramienta que la emplee le permitirá a quien se sirva de ella adentrarse en el ámbito más oculto de cada ser humano, asimismo, podría afirmarse que, a través de ella, es posible vulnerar la intimidad del trabajador. (Mercader Uguina, 2020, p. 1). Esto muestra que, aunque los sistemas biométricos tienen funciones empresariales legítimas (como la verificación de identidad, la seguridad y el control horario), su uso conlleva un alto riesgo de interferir en los derechos básicos de los trabajadores, sobre todo cuando este tratamiento es constante y obligatorio durante el vínculo de subordinación.

Teniendo ello en consideración, destacamos que los *wearables*, dispositivos tecnológicos que los empleados llevan en su cuerpo y que posibilitan el monitoreo de variables conductuales y fisiológicas en tiempo real, son un ejemplo representativo de datos biométricos empleados en el entorno laboral. Estas herramientas han proliferado rápidamente en distintos sectores productivos, en particular en la industria minera, donde las tareas de alto riesgo requieren mecanismos de seguridad y prevención de accidentes más sólidos.

Según Taco (2022), los *wearables* presentan las siguientes características:

Estos dispositivos son utilizados por usuarios de manera externa, de ahí el término wearable, que en español significa “llevable”. Permiten que el usuario pueda interactuar con sus registros personales y, a su vez, intercambiar o compartir datos como estos: **frecuencia cardíaca, hábitos de sueño, geolocalización, parámetros fisiológicos, parámetros clínicos, hábitos alimenticios y calendario** (p.215). (Énfasis agregado)

Para Klopfenstein et al. (2019), los dispositivos tecnológicos anteriormente mencionados son un instrumento de detección, comunicación y rastreo de la salud y el estado físico de las personas, los cuales tienen la capacidad de recopilar, procesar y transmitir los datos (p. 510). Sobre este punto, la OIT (2025) señala que estos dispositivos *"registran constantes fisiológicas (frecuencia cardíaca, temperatura corporal) y riesgos ambientales para proporcionar alertas inmediatas"* (p. 11).

Asimismo, Dios (2022) advierte que *"los wearables pueden monitorizar nuestra salud y nuestro estilo de vida sin perjuicio para la salud y la seguridad"* (p. 168). A continuación, presentamos un breve resumen que define las principales características de los *wearables* o la tecnología vestible.

<b>Wearables/ tecnología vestible / ropa inteligente</b>	
<b>Concepto</b>	Dispositivos electrónicos que se incorporan en el cuerpo del usuario que permiten la recopilación, procesamiento y transmisión de datos en tiempo real, vinculados con la salud, rendimiento físico o ubicación.
<b>Diseño</b>	Se incorporan y pueden ser usados en el cuerpo (relojes o <i>smartwatches</i> , pulseras, gafas, anillos).
<b>Funciones</b>	Recolección y procesamiento de datos biométricos o ambientales en tiempo real.

<b>Componentes típicos</b>	Microprocesadores, baterías, sensores de pulso, Sistema de Posicionamiento Global (GPS) o conexiones inalámbricas como el <i>Bluetooth</i> y <i>Wi-Fi</i> .
<b>Ámbitos de aplicación</b>	Focalizados en el ámbito de la salud y el bienestar, seguimiento de la actividad física, sueño, ritmo cardíaco, etc.

**Nota.** Elaboración propia.

Al respecto, Montoro Osuna y Ávila Gutiérrez (2019) destacan que *"los dispositivos wearables [...] permiten implementar modelos de prevención en tiempo real"* (p. 4). Siendo ello así, los *wearables* representan un rol importante en la gestión de seguridad y salud en el trabajo y en la prevención de riesgos laborales, pues permiten recopilar datos fisiológicos importantes para gestionar y alertar cualquier incidente o accidente en tiempo real de forma predictiva.

Ahora bien, tomando en consideración que los *wearables* recopilan información de vital importancia en tiempo real, debemos destacar que dicha característica dota de predictibilidad a dichos aparatos al momento de ser usados en el ámbito laboral. Por ejemplo, si los datos que arrojan los *wearables* sobre un trabajador X nos demuestran que es una persona con malos ciclos de sueño, ello impactará ineludiblemente en su desempeño laboral, más aún si hablamos de sectores de riesgo como la minera en la que se trabaja con maquinarias pesadas o a cargo de herramientas sumamente peligrosas para las cuales se necesita estar en óptimas condiciones.

Inclusive, actualmente algunos dispositivos electrónicos ahora permiten medir el nivel de estrés de las personas, por lo que las empresas podrían contar con data precisa que cuantifique los riesgos psicosociales a fin de que gestionen estrategias de prevención de riesgos psicosociales y promoción de la salud

mental. Esta particularidad permite gestionar mejor los accidentes laborales por fatiga y, sobre todo, se centra en su prevención.

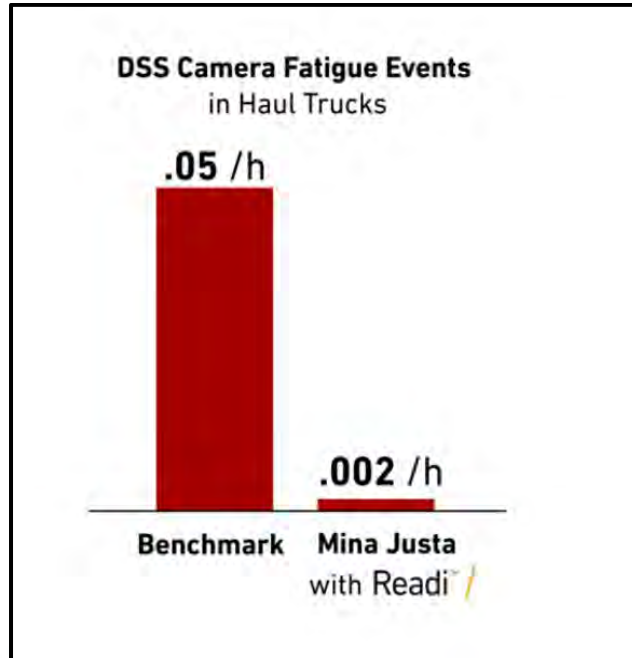
En el caso peruano, *Fatigue Science*, proveedor líder de soluciones de gestión de la fatiga, elaboró un programa integral de gestión de la fatiga con apoyo tecnológico - de forma específica estamos hablando del uso dispositivos conocidos como smartwatches o relojes inteligentes - para una de las mineras más importantes del país.

Estamos hablando de la Mina Justa de Marcobre, la cual desde el 2019 utiliza “Readi”, una plataforma de gestión predictiva de la fatiga” en la Mina Justa o, en otras palabras, implementó un sistema de Gestión de Fatiga con el objetivo de asegurar el bienestar e integridad de sus trabajadores bajo el lema “El cero accidente es posible” (2023).

Este sistema consiste en el uso de dispositivos conocidos como Readiband o Readiwatch junto con los *wearables*, los cuales sirven para lo siguiente:

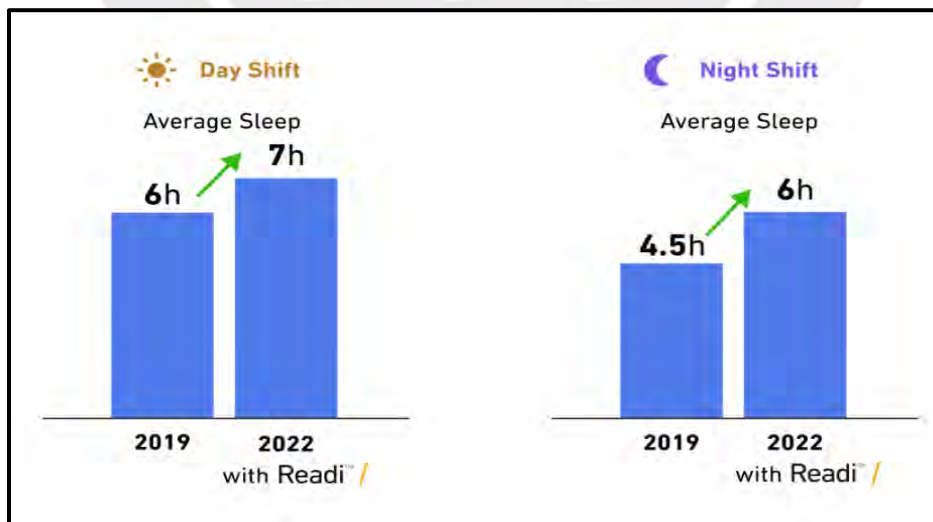
Mejorar la concienciación personal sobre la fatiga entre sus operarios, así como para fomentar y mejorar la disciplina del sueño. El despliegue de Readi ha tenido un profundo impacto en las vidas de los operarios de los camiones mineros de Mina Justa, que ahora conocen mejor sus patrones de sueño y son conscientes a diario de sus niveles personales de fatiga. *Fatigue Science* (2023).

La minera Marcobre a finales de 2022 registró apenas 0,002 incidentes de fatiga por hora trabajada frente al resto de empresas, mientras, lo que indica un incidente de fatiga cada 500 horas. De esta manera, se demuestra que esta mejora es, en parte, al enfoque de Readi en la gestión proactiva de la fatiga y al apoyo proporcionado por los controladores de fatiga, conforme se aprecia en el siguiente gráfico.



**Nota.** Imagen extraída de Fatigue Science (2023).

Asimismo, el uso de ReadiScore garantiza que los trabajadores alcancen el nivel mínimo de alerta antes de iniciar su jornada laboral. Esto ha mejorado sus hábitos de sueño, aumentando su descanso promedio en turnos de día como de día. De esta manera, se reduce el riesgo de accidentes laborales por fatiga laboral. Veamos:



**Nota.** Imagen extraída de Fatigue Science (2023).

En conclusión, el caso de Marcobre nos demuestra cómo el uso de tecnologías predictivas como el Readi junto con aparatos electrónicos como los wearables permite contribuir con la gestión de fatiga en el sector minero peruano. Marcobre es un caso importante porque demuestra que han logrado reducir los eventos de fatiga, mejorar la calidad de sueño y vida de sus trabajadores y fomentar una cultura de seguridad y salud en el trabajo.

#### **IV. NORMATIVA PERUANA QUE REGULA Y PROMUEVE EL USO DE LA INTELIGENCIA ARTIFICIAL**

Antes de la promulgación de este marco normativo, las tecnologías de control en el ámbito laboral —videovigilancia, registro biométrico, algoritmos de gestión— se utilizaban sin un estándar específico de transparencia o rendición de cuentas. No obstante, con la incorporación al marco normativo de la Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, y su Reglamento, aprobado por el Decreto Supremo N 115-2025-PCM se introdujo un marco vinculante para el diseño y uso de sistemas de inteligencia artificial en el país, que alcanza de manera directa a las relaciones de trabajo tanto en el sector público como en el privado.

Siendo ello así, la presente ley se enmarca en el Sistema Nacional de Transformación Digital (SNTD) y otorga a la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD), la autoridad técnico-normativa para dirigir, evaluar y supervisar el uso de la IA y otras tecnologías emergentes en los sectores público y privado.

Esto quiere decir que la legislación consolida un modelo de gobernanza tecnológica donde la Secretaría de Gobierno y Transformación Digital de la PCM asume rol rector y técnico-normativo, facultados por el artículo 4 de la Ley y los artículos 8 y 9 del Reglamento, lo que implica que las decisiones empresariales soportadas en IA —procesos de reclutamiento, segmentación de candidatos, evaluación del desempeño, asignación de turnos, monitoreo de productividad o

videovigilancia inteligente— dejan de ser un ámbito “neutro” de gestión interna para someterse a estándares públicos de legalidad, transparencia, supervisión humana, rendición de cuentas y respeto de derechos fundamentales.

En ese sentido, el empleador que incorpora sistemas algorítmicos pasa a estar obligado a demostrar que sus herramientas no producen discriminación directa o indirecta, que el tratamiento de datos personales es compatible con la Ley N.º 29733, que existe intervención humana eficaz en decisiones con impacto significativo en la situación del trabajador (promoción, sanción, despido, asignación de riesgos) y que se han adoptado medidas proporcionales de seguridad y fiabilidad conforme a los principios rectores del Reglamento (no discriminación, privacidad, transparencia, supervisión humana, rendición de cuentas, estándares basados en riesgos).

De este modo, la IA en el trabajo deja de ser solo un instrumento de eficiencia para convertirse en un objeto de control jurídico reforzado: cualquier decisión laboral automatizada debe ser explicable, verificable y objetivamente justificada, bajo riesgo de configurar actos de discriminación, vulneración a la intimidad, afectación a la dignidad del trabajador o uso abusivo del poder de dirección.

#### **IV.1. PRINCIPIOS RECTORES DE LA INTELIGENCIA ARTIFICIAL APLICADOS AL ÁMBITO LABORAL**

De esta forma, el Reglamento de la Ley N.º 31814 implementa un marco de principios rectores que orientan el uso de la inteligencia artificial bajo parámetros éticos, jurídicos y sociales. Estos principios buscan garantizar que la tecnología se utilice al servicio de la persona y no en su perjuicio, asegurando la tutela de los derechos fundamentales en el entorno laboral digital.

A continuación, se presenta una tabla explicativa con los principios rectores y su aplicación específica en el contexto laboral:

<b>Principio</b>	<b>Base normativa</b>	<b>Contenido</b>	<b>Aplicación en el ámbito laboral</b>
<b>No discriminación</b>	Art. 7 inc. a) del Reglamento	Obliga a prevenir, mitigar y corregir sesgos o resultados discriminatorios generados por sistemas de IA.	Evita que algoritmos de selección o evaluación excluyan por género, edad, discapacidad o afiliación sindical. Promueve procesos de contratación y promoción equitativos.
<b>Privacidad de los datos personales</b>	Art. 7 inc. b) del Reglamento	Impone el respeto irrestricto a la privacidad y protección de datos personales mediante medidas técnicas y legales.	Protege la información biométrica y de rendimiento laboral; prohíbe usos desproporcionados o sin consentimiento del trabajador.
<b>Protección de derechos fundamentales</b>	Art. 7 inc. c) del Reglamento	Garantiza el respeto a la dignidad, igualdad, intimidad y bienestar humano en el uso de la IA.	Evita decisiones automatizadas que vulneren derechos constitucionales o laborales. Refuerza el principio protector del Derecho del Trabajo.
<b>Respeto del derecho de autor y</b>	Art. 7 inc. d) del Reglamento	Exige respetar la propiedad intelectual de	Protege los contenidos generados por trabajadores o

<b>derechos conexos</b>		los creadores en el uso y desarrollo de IA.	desarrolladores frente al uso indebido de obras o códigos.
<b>Seguridad, proporcionalidad y fiabilidad</b>	Art. 7 inc. e) del Reglamento	Obliga a que los sistemas sean seguros, proporcionales y confiables, con salvaguardas según el nivel de riesgo.	Asegura que los sistemas de control laboral (monitoreo, videovigilancia, registro biométrico) funcionen de forma segura y no invasiva.
<b>Sensibilización y educación en IA</b>	Art. 7 inc. f) del Reglamento	Promueve la alfabetización digital y la comprensión del impacto de la IA.	Incentiva la capacitación continua de los trabajadores para adaptarse a la transformación digital y prevenir brechas tecnológicas.
<b>Sostenibilidad</b>	Art. 7 inc. g) del Reglamento	Exige analizar los impactos humanos, sociales, económicos y ambientales del uso de IA.	Impulsa políticas laborales sostenibles y responsables, priorizando prácticas tecnológicas que respeten el entorno y el bienestar humano.
<b>Supervisión humana</b>	Art. 7 inc. h) del Reglamento	Todo sistema basado en IA debe contar con revisión y control humano efectivo.	Garantiza que las decisiones sobre evaluación, sanción o despido sean verificadas por personas y no

			exclusivamente por algoritmos.
<b>Transparencia</b>	Art. 7 inc. i) del Reglamento	Los sistemas deben ser explicables, accesibles y comprensibles para usuarios y autoridades.	El trabajador tiene derecho a conocer cómo opera la IA que incide en su desempeño o evaluación, reforzando el principio de motivación y defensa.
<b>Rendición de cuentas</b>	Art. 7 inc. j) del Reglamento	Los actores involucrados asumen responsabilidad por los efectos de la IA, positivos o negativos.	Permite exigir responsabilidad al empleador o desarrollador ante daños por decisiones automatizadas injustas o discriminatorias.
<b>Desarrollo ético para una IA responsable</b>	Art. 7 inc. k) del Reglamento	Promueve un enfoque ético centrado en el respeto de los derechos humanos y la dignidad.	Exige políticas empresariales de ética digital y mecanismos internos de control de integridad tecnológica.
<b>Estándares de seguridad basados en riesgos</b>	Art. 7 inc. l) del Reglamento	Obliga a identificar amenazas y vulnerabilidades según el nivel de riesgo del sistema de IA.	Impone la evaluación preventiva de riesgos laborales tecnológicos y la adopción de protocolos de ciberseguridad.

Los doce principios rectores establecen un modelo de gobernanza tecnológica humanista, en el cual la inteligencia artificial trasciende su función como herramienta técnica para convertirse en un objeto jurídico que se encuentra sujeto a los controles de legalidad, ética y proporcionalidad. En el contexto laboral, los principios mencionados guían la implementación responsable de herramientas algorítmicas, estableciendo que toda utilización de inteligencia artificial debe:

- Proteger la dignidad y la intimidad del trabajador
- Evitar la discriminación indirecta derivada de sesgos en los datos o algoritmos.
- Asegurar transparencia y control humano efectivo sobre cualquier decisión automatizada.
- Garantizar la rendición de cuentas empresarial ante posibles vulneraciones de derechos.

Así, el Decreto Supremo N.º 115-2025-PCM transforma el uso de la IA en un espacio de responsabilidad compartida entre el Estado, las empresas y los trabajadores. Así, podemos observar cómo coloca como prioridad al trabajador de cualquier arbitrariedad y al empleador como responsable del poder de dirección digital.

#### **IV.2. RIESGOS LABORALES DERIVADOS DEL USO DE INTELIGENCIA ARTIFICIAL**

La utilización de tecnologías de control en el ámbito laboral representa un desafío legal significativo en la actualidad. Esto se debe a que los procedimientos de supervisión empresarial han adquirido una mayor complejidad, impulsados por la implementación de sistemas digitales que trascienden la simple observación física del empleado.

Entre los aspectos relevantes se encuentran los siguientes: i) la vigilancia por video en los lugares de trabajo, que permite el monitoreo continuo del comportamiento del personal; ii) la gestión de datos biométricos para el registro de la asistencia y las horas laboradas, lo que conlleva la manipulación de información altamente sensible; y iii) la implementación de algoritmos y decisiones automatizadas en la administración laboral, que afectan de manera directa la evaluación del rendimiento, la asignación de tareas y la continuidad del vínculo laboral.

Con la implementación del Reglamento de la Ley N.º 31814, estos mecanismos no son evaluados únicamente en términos de su legalidad o proporcionalidad; además, se les puede medir a través de una clasificación de riesgos, considerando el efecto que tienen sobre los derechos fundamentales de los trabajadores.

Esta categorización —que distingue entre uso indebido, uso de riesgo alto y riesgo aceptable— posibilita definir el grado de intervención estatal y empresarial que se necesita, así como las responsabilidades de transparencia, supervisión humana y rendición de cuentas que tiene quien crea o ejecuta sistemas de inteligencia artificial en la esfera laboral.

A continuación, presentamos la clasificación de riesgos conforme al siguiente cuadro:

Nivel de riesgo	Definición	Sistemas basados en IA
<b>Uso indebido</b>	Cuando el uso de IA puede impactar de manera irreversible,	<ul style="list-style-type: none"> <li>- Analizar, clasificar o inferir datos sensibles de las personas sobre la base de sus datos biométricos (deducir su orientación sexual u opiniones políticas).</li> <li>- Evaluar o clasificar personas naturales o</li> </ul>

	<p>significativa y negativa los derechos fundamentales o el bienestar de las personas.</p>	<p>colectivos cuando genere o contribuya a resultados discriminatorios o desproporcionados que vulneren derechos humanos.</p> <ul style="list-style-type: none"> <li>- Realizar identificación biométrica en tiempo real para la categorización de personas naturales en espacios públicos (salvo que tenga como fin únicamente la autenticación de la identidad o una investigación preliminar de delitos graves).</li> </ul>
<p><b>Uso de riesgo alto</b></p>	<p>Si bien su uso puede suponer un riesgo para los derechos fundamentales, puede ser usado bajo determinadas condiciones y/o controles.</p>	<ul style="list-style-type: none"> <li>- Determinar la evaluación crediticia de personas (salvo que se use la IA para detectar fraude).</li> <li>- Determinar el acceso a servicios de salud y complementarios, así como orientar la evaluación, diagnóstico o pronóstico del estado de salud de las personas.</li> <li>- Determinar procesos de selección, evaluación, contratación y cese de trabajadores.</li> </ul>
<p><b>Riesgo aceptable</b></p>	<p>Todos los sistemas basados en IA que no calcen en las clasificaciones previamente señaladas.</p>	<ul style="list-style-type: none"> <li>- Herramientas administrativas o logísticas.</li> <li>- Sistemas que no procesan datos personales ni influyen directamente en derechos laborales.</li> </ul>

Así, el derecho del trabajo incluye una metodología de gestión del riesgo tecnológico que se ajusta a los principios de precaución, debida diligencia y proporcionalidad. En este sistema, cada instrumento de control digital debe ser

examinado en función de su capacidad para impactar la intimidad, la igualdad, la dignidad y la estabilidad laboral del empleado.

## **V. PROTECCIÓN DE LOS DERECHOS LABORALES EN EL ENTORNO DIGITAL**

En el contexto del trabajo digitalizado, el poder de dirección del empleador conserva su esencia como manifestación del principio de subordinación laboral, pero su ejercicio enfrenta hoy límites más complejos derivados del uso intensivo de tecnologías de información, control y vigilancia.

En ese sentido, el poder de dirección del empleador no puede menoscabar otros derechos fundamentales; es decir, su uso no es irrestricto y tiene que respetar ciertos límites. Tanto es así que goza de protección constitucional conforme al artículo 23 de la Constitución Política del Perú, que señala que “ninguna relación laboral puede limitar el ejercicio de los derechos constitucionales, ni desconocer o rebajar la dignidad del trabajador”.

Los referentes comparados proporcionan criterios valiosos para organizar el poder de dirección en términos digitales. El principio de proporcionalidad se establece como la regla de oro en primer lugar: ante tensiones entre los derechos fundamentales y el control, “es necesario [...] superar el principio de proporcionalidad, donde es fundamental que las partes muestren reciprocidad en la relación jurídica” (Aragüez, 2021, p. 454).

En segundo lugar, los estándares de transparencia e información previa —con base en la Ley N.º 29733, Ley de Protección de Datos Personales (LPDP), y su reglamento, el Decreto Supremo N.º 003-2013-JUS (RLPDP)— exigen las siguientes obligaciones y derechos en cuanto al tratamiento de los datos personales de los trabajadores. Conforme puede advertirse en el siguiente cuadro (Bárraga, 2025. p. 72):

Concepto	Contenido
Principios generales (Art. 4, 5, 6 y 7 LPDP)	<b>Legalidad:</b> Su tratamiento debe ser conforme a la ley y se prohíbe su recopilación fraudulenta, desleal e ilícita.
	<b>Consentimiento:</b> Para su tratamiento debe existir el consentimiento del titular.
	<b>Proporcionalidad:</b> El tratamiento de datos personales debe ser adecuado, relevante y no debe exceder su finalidad.
	<b>Finalidad:</b> Tiene que ser determinada, explícita y lícita y no pueden extender su finalidad que no haya sido comunicada.
Derechos del titular (Art. 18, LPDP)	El titular tiene derecho a ser informado de forma detallada, sencilla, expresa, inequívoca y de manera previa sobre la finalidad para la que sus datos personales serán tratados.
Límites del consentimiento (Art. 14, inciso 5, LPDP)	Existen supuestos en los cuales no se requiere el consentimiento del titular, por ejemplo, cuando los datos personales sean necesarios para ejecución de una relación contractual en la que el titular de los datos personales es parte o cuando se derive de una relación profesional y sea necesario para su adecuado cumplimiento o desarrollo.
Derechos fundamentales (Art. 13, incisos 1 e inciso 2, LPDP)	<b>Alcances:</b> El tratamiento debe respetar los derechos fundamentales del titular y los derechos que la ley le confiere. <b>Límites:</b> Las restricciones al derecho fundamental de protección de datos personales solo pueden ser establecidas por ley y deben respetar su contenido esencial.

Desde una perspectiva jurídica, Carmen Sáez Lara (2015) advierte que *"el poder de dirección del empleador no es absoluto y debe armonizarse con el respeto a los derechos fundamentales del trabajador"* (p. 32). Esto implica que toda

implementación tecnológica debe adherirse al principio de proporcionalidad y garantizar el consentimiento informado del trabajador.

En este contexto, es importante señalar que, aunque estos dispositivos ofrecen beneficios considerables tanto para los trabajadores como para los empleadores, su uso sin una regulación adecuada podría resultar en una intrusión excesiva y poner en riesgo los derechos fundamentales de los trabajadores. En consecuencia, la normativa debe asegurar un equilibrio adecuado entre la utilización de estas tecnologías y la protección de los derechos mencionados.

En esa misma línea, Puntriano establece que los derechos fundamentales del trabajador dentro del vínculo laboral funcionan como un límite al derecho constitucional a la libertad de empresa del empleador, por lo que es necesario realizar una validez del ejercicio del poder de (control) vigilancia empresarial (2020, p. 731). De esta forma, los límites a la facultad de fiscalización dentro del marco de las nuevas tecnologías de la información, como el monitoreo laboral mediante IA y dispositivos tecnológicos, son la afectación a derechos fundamentales como la imagen, la intimidad, la dignidad y la protección de datos personales (De las Casas, 2012, p. 70).

Asimismo, se advierte que los límites que debe observar el empleador respecto al uso del monitoreo laboral mediante inteligencia artificial dentro del centro de trabajo comprenden lo siguiente:

- Respetar los derechos fundamentales del trabajador (dignidad, intimidad, protección de datos personales, imagen y voz.
- Los trabajadores deben estar debidamente informados de la finalidad en cuanto al uso de IA.
- Se debe priorizar que el uso de la IA sean los menos lesivos a los derechos de los trabajadores.

Conforme se observa, en el caso peruano, la legislación laboral y la normativa de protección de datos personales —principalmente la Ley N.º 29733, Ley de Protección de Datos Personales, y su Reglamento— establecen principios y obligaciones en materia de tratamiento de datos personales.

Finalmente, la doctrina y jurisprudencia comparadas —incluida la europea— subrayan que el control tecnológico no puede vaciar los derechos del trabajador “como ciudadano”, debiendo ponderarse libertades económicas y derechos fundamentales, con modulaciones “en la medida estrictamente imprescindible” para el desenvolvimiento productivo (Aragüez, 2021, p. 455). A los parámetros mencionados se incorporan marcos de referencia contemporáneos, tales como el Reglamento General de Protección de Datos de la Unión Europea y el Reglamento de Inteligencia Artificial de la Unión Europea. Estos marcos refuerzan principios fundamentales como la minimización de datos, la transparencia, la supervisión humana y la no discriminación en los sistemas de gestión algorítmica.

## **VI. CONCLUSIONES**

- La transformación digital se ha desarrollado con rapidez, lo cual ha posibilitado que los poderes de dirección del empleador crezcan considerablemente, ya que han pasado de un ámbito físico y perceptible a uno virtual donde la supervisión es continua y automatizada. Este cambio implica la necesidad de una reinterpretación del *ius variandi*, la cual debe llevarse a cabo con un estricto cumplimiento del principio de proporcionalidad, con el fin de evitar interferencias excesivas en los derechos fundamentales del empleado.
- La introducción de tecnologías como el control biométrico, la videovigilancia inteligente y los sistemas algorítmicos de administración proporciona ventajas en el ámbito laboral. No obstante, su

implementación conlleva riesgos legales significativos, como violaciones al derecho a la privacidad, discriminación por sesgos algorítmicos y decisiones automatizadas poco transparentes, que pueden resultar en abusos del poder directivo.

- El uso de datos biométricos y la vigilancia algorítmica requieren un procesamiento exhaustivo de información muy sensible, lo cual demanda garantías mejoradas como la supervisión humana eficaz, la transparencia, la reducción de datos y las medidas legales y técnicas. En sectores de alto riesgo, como el de la minería, la implementación de dispositivos portátiles ha demostrado ser eficaz en la prevención de accidentes.
- El establecimiento de deberes concretos para el desarrollo y la utilización de la inteligencia artificial en los sectores público y privado mediante la Ley N.º 31814 y su reglamento ha sido un hito que ha impactado en los trabajadores, empleadores y el Estado; sin embargo, aún hay existe diversos retos a afrontar que excede lo establecido en la recién legislación.

## BIBLIOGRAFÍA

Aragüez Valenzuela, L. (2021). Debates emergentes en materia laboral y de privacidad: sistemas de videovigilancia, algoritmos digitales e identificación biométrica de la persona trabajadora. *THEMIS Revista De Derecho*, (79), 451–466.

Bárraga Ochoa, A. M. (2025). Informe jurídico sobre la Resolución recaída en el Expediente Casatorio 8273-2018-LIMA [Trabajo académico, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. <http://hdl.handle.net/20.500.12404/31478>

Blancas, C. (2007). El acoso moral en la relación de trabajo. Lima: Palestra Editores.

Boza, G. (2020). Derecho del trabajo. Fondo Editorial PUCP.

Constitución Política del Perú. (1993).

De las Casas de la Torre Ugarte, O. (2012). La protección de los derechos fundamentales laborales. *Soluciones Laborales*, (56), 70-78.

Decreto Legislativo N.º 728. Ley de Productividad y Competitividad Laboral. (1991). Diario Oficial El Peruano, 27 de noviembre de 1991.

Decreto Supremo N.º 003-2013-JUS. Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales. (2013). Diario Oficial El Peruano, 22 de mayo de 2013.

Decreto Supremo N.º 115-2025-PCM. Reglamento de la Ley N.º 31814. (2025). Diario Oficial El Peruano, 29 de enero de 2025.

Dios, I. S. F. (2022). Inteligencia artificial y entornos de trabajo robotizados: estándares de seguridad y salud en el trabajo. *Labour 2030*.

Fajardo-López, D. J., Fracica-González, Y. J., Alarcón-Sierra, I. D., Rincón-Romero, P. A., Rico-Pillajo, L. D., & Jiménez-Sánchez, Y. C. A. (2023). Inteligencia artificial aplicada a la Seguridad y Salud en el Trabajo: Revisión narrativa de la literatura. Universidad Cooperativa de Colombia.

Fatigue Science. (2023, 21 de abril). *VIDEO: Marcobre's Mina Justa mine uses Readi to reduce fatigue events, improving safety and productivity* [Entrada de blog]. Fatigue Science. <https://fatiguescience.com/es/blog/video-marcobres-mina-justa-mine-uses-readi-to-reduce-fatigue-events-improving-safety-and-productivity>

Fiberlux. (2020). *Nuevas tendencias de la inteligencia artificial en cámaras de video vigilancia*. <https://fiberlux.pe/nuevas-tendencias-de-la-inteligencia-artificial-en-camaras-de-video-vigilancia/>

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*. Dykinson.

Klopfenstein, L. C., Delpriori, S., Aldini, A., & Bogliolo, A. (2019). "Worth one minute": An anonymous rewarding platform for crowd-sensing systems. *Journal of Communications and Networks*, 21(5), 509–520.

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

Ley N.º 31814. Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. (2024). Diario Oficial El Peruano, 7 de junio de 2024.

Loratech. (2024). *Videovigilancia con IA en Perú: seguridad que piensa por sí misma*. <https://www.loratech.pe/videovigilancia-con-ia-en-peru-seguridad-que-piensa-por-si-misma/>

Macías García, M. D. C. (2022). La inteligencia artificial para el entorno laboral: Un enfoque en la predicción de accidentes. *Estudios en Relaciones Industriales y Psicología del Trabajo*, 7(1), 85–101.

Mercader Uguina, J. R. (2020). Datos biométricos en los centros de trabajo. *Trabajo y Derecho*, (11), 1–23. Wolters Kluwer.

Montoro Osuna, E. M., & Ávila Gutiérrez, M. (2019). La digitalización de la prevención de riesgos laborales. Una aproximación para la PRL 4.0. AEIPRO.

Organización Internacional del Trabajo (OIT). (2025). Día Mundial de la Seguridad y Salud en el Trabajo: Materiales promocionales. Ginebra: OIT.

Puntriano Rosas, C. A. (2020). La videovigilancia en el ámbito laboral. En M. Y. Matos Zegarra (Ed.), *IX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*. Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social, 721-747.

Ramos, X. I. (2019). Los límites a la videovigilancia en el ejercicio de las facultades fiscalizadoras del empleador en el Perú [Trabajo Académico para optar por el título de Segunda Especialidad en Derecho del Trabajo y de la Seguridad Social]. Obtenido de Repositorio Digital de Tesis y Trabajos de Investigación PUCP: <http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/16006>

Rodríguez-Piñero Royo, M. (2024). La videovigilancia en el trabajo en tiempos de inteligencia artificial. *LABOS. Revista de Derecho del Trabajo y Protección Social*, 5, 68–82.

Taco Jimenez, A. R. (2022). Dispositivos *wearables* y los riesgos a la privacidad: Una revisión de la literatura. *Interfases*, (16), 213–229.

Torres Cadillo, R. (2023). Los riesgos y los desafíos que enfrentan los trabajadores frente al uso de la inteligencia artificial en el trabajo. *Revista de Derecho Procesal del Trabajo*, 6(7), 289–313.

Toyama Miyagusuku, J., & Girao La Rosa, J. (2014). GPS Laboral: La facultad de Fiscalización del Empleador a partir de las Nuevas Tecnologías de la Información. *IUS ET VERITAS*, 24(49), 176-189.

Tribunal Constitucional del Perú. (2010). Sentencia recaída en el Exp. N.º 01405-2010-PA/TC, 12 de agosto de 2010.

Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD). Diario Oficial de la Unión Europea.

Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act). Diario Oficial de la Unión Europea.

Vílchez Garcés, L. (2020). Nuevas tecnologías y poder de dirección: la fiscalización laboral en la era de la inteligencia artificial. En Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social (Ed.), *IX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social* (pp. 645–683). Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social.