

IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO LABORAL: BENEFICIOS, RIESGOS Y DESAFÍOS LEGALES EN LA GESTIÓN DE TRABAJADORES

LUIS MIGUEL MEDINA GUTIÉRREZ

Abogado y Maestría en Derecho del Trabajo por la Universidad de San Martín de Porres (USMP) y MBA Centrum/ Especialista en Derecho del Trabajo por la Universidad de Castilla la Mancha y Universidad de Salamanca. Profesor de Derecho del Trabajo de la USMP/Gerente Relaciones Laborales -Claro Perú

I. INTRODUCCIÓN

En la era actual, la IA se posiciona como un componente esencial de la quinta revolución industrial, al igual que lo fueron la electricidad y el internet en su momento. Este fenómeno, impulsado por la integración de tecnologías avanzadas como *Big Data*, *Machine Learning* e internet de las cosas, está transformando diversos sectores, incluido el ámbito laboral. La IA generativa, en particular, se ha convertido en un motor de cambio, no solo optimizando procesos, sino también generando contenido nuevo y mejorando la eficiencia en múltiples industrias.

Así como la máquina de vapor impulsó la revolución industrial, la electricidad la producción y la calidad de vida, la IA está moldeando el futuro del trabajo. Aunque el avance de esta tecnología varía según el poder económico y el desarrollo tecnológico de cada país, su impacto se anticipa tan profundo y generalizado como el de sus predecesoras tecnológicas.

Este artículo analiza el impacto de la IA en el entorno laboral, enfocándose en sus aplicaciones prácticas y los desafíos regulatorios que plantea. Se examinan los efectos de la IA en la organización, control de los trabajadores, así como en la seguridad y salud en el trabajo. Además, se destaca cómo los principios de razonabilidad, proporcionalidad, minimización de datos personales, explicabilidad y supervisión humana pueden guiar la implementación de la IA dentro de la relación laboral.

1. Una aproximación a la inteligencia artificial

- a) Origen y evolución de la IA: La evolución de la IA ha sido notable desde sus inicios en los años 50, con la teoría de las máquinas de Turing y los primeros programas de ajedrez. Durante los años 60 y 70, surgieron los sistemas expertos, seguidos en los 80 por un creciente interés en redes neuronales y aprendizaje automático con limitaciones tecnológicas propias de la época. El avance en hardware

y la disponibilidad de grandes volúmenes de datos en los 2000 impulsaron el aprendizaje profundo, revolucionando áreas como el reconocimiento de voz y la visión por computadora. Hoy en día, la IA está integrada en la vida cotidiana, desde asistentes virtuales, *chatbots* hasta vehículos autónomos, con continuos avances en procesamiento del lenguaje natural e IA generativa (Russell & Norvig, 2021).

- b) Definiciones de la IA: La IA se entiende comúnmente como una tecnología capaz de imitar el razonamiento humano mediante el análisis de grandes volúmenes de datos a través de algoritmos informáticos. Según Rouhiainen (2018, pp. 17-19), la IA es la capacidad de las máquinas para utilizar algoritmos y aprender de los datos, permitiéndoles tomar decisiones de manera similar a los humanos. IBM (2024) la describe como una tecnología que permite a las computadoras imitar la inteligencia humana y resolver problemas, operando de manera autónoma o en conjunto con otras tecnologías como sensores y robótica.

En esa línea, la Organización para la Cooperación y el Desarrollo Económicos, OCDE (2024) define la IA como “un sistema basado en una máquina que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar resultados como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales”. El Reglamento de la Unión Europea 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024, que establece normas armonizadas en materia de IA publicado el 12 de julio de 2024¹ en el Diario Oficial de la UE (RIAUE) define al sistema de IA como: “*un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*”.

¹ Boletín Oficial del Estado de España: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079>. Vigente desde 01 de agosto de 2024. Aplicable como regla general a los 24 meses de su entrada en vigor. Excepciones: Prácticas prohibidas a partir de los 6 meses de entrada en vigor. Gobernanza, sanciones, confidencialidad y otros a los 12 meses de entrada en vigor. Reglas de clasificación de los sistemas de alto riesgo y obligaciones a los 36 meses de su entrada en vigor.

En Perú, la Ley N° 31814, que promueve el uso de la IA para el desarrollo económico y social, define un sistema basado en IA como un “*sistema electrónico-mecánico que puede, para una serie de objetivos definidos por humanos, hacer predicciones, recomendaciones o tomar decisiones, influenciando ambientes reales o virtuales*”. Un algoritmo, según esta ley, es una “*secuencia de instrucciones y de conjuntos ordenados y finitos de pasos para resolver un problema o tomar una decisión*”.

A partir de estas definiciones, podemos sostener que la IA se entiende como una tecnología que permite a las máquinas en base a algoritmos tomar decisiones, realizar predicciones o recomendaciones, y ejecutar tareas mediante el análisis de datos, imitando la inteligencia humana. Los sistemas de IA operan con distintos niveles de autonomía y son capaces de influir en entornos tanto físicos como virtuales.

c) Tipos de IA y su impacto en la sociedad: Existen diversas taxonomías de la IA que permiten comprender mejor sus aplicaciones. En este trabajo, propongo una clasificación basada en su funcionalidad. La IA se divide en dos tipos: i) basada en reglas predefinidas para la toma de decisiones, sobre la que no ahondaremos; y ii) basada en aprendizaje automático o *Machine Learning*. Dentro del aprendizaje automático, encontramos tres subcategorías: a) supervisado², donde se entrena al sistema de IA con datos etiquetados; b) no supervisado, que identifica patrones en datos no etiquetados; y c) por refuerzo, que toma decisiones optimizadas mediante un sistema de recompensas y castigos. AlphaGo es un ejemplo destacado de aprendizaje por refuerzo. Desarrollado por DeepMind, AlphaGo utilizó redes neuronales profundas y jugó miles de partidas contra sí mismo, mejorando su estrategia con cada partida. Esto le permitió derrotar al campeón europeo de Go, Fan Hui, y alcanzar un hito significativo en la IA (David Silver et al., 2016, p. 484-489)

2 Un ejemplo de aprendizaje automático supervisado es cuando la IA aprende a distinguir entre un gato y un perro en una imagen. Se entrena con un gran conjunto de imágenes representativas y de alta calidad, donde se identifican gatos y perros, para que pueda diferenciarlos. Inicialmente, se le indica cuál es un perro o un gato, lo que permite que las capas de la IA deduzcan patrones, entendidos como conjuntos de rasgos y puntos que forman cada imagen. Cada capa se enfoca en una característica específica, como formas, colores o particularidades distintivas. Así, el modelo puede predecir, a partir de una nueva imagen no utilizada en el entrenamiento, si lo que aparece es un gato o un perro. La precisión del modelo depende de la cantidad, calidad y diversidad de los datos de entrenamiento.

El aprendizaje automático, tiene como subcampo al aprendizaje profundo (*deep learning*), que emplea redes neuronales para tareas complejas como el reconocimiento de voz y el procesamiento del lenguaje natural. Por ejemplo, Facebook realiza 4,500 millones de traducciones automáticas diarias utilizando esta tecnología (Rouhiainen, 2018). A su vez, la IA generativa, una avanzada forma de aprendizaje profundo utiliza métodos supervisados, no supervisados y por refuerzo para generar contenido como textos, imágenes, música y otros de manera similar a un humano. Utiliza arquitecturas de redes neuronales profundas y modelos de lenguaje natural a gran escala para procesar y generar lenguaje y otros tipos de datos (Casar, 2023).

Los diversos tipos de IA impactan en numerosos sectores en la vida cotidiana. Asistentes virtuales como Siri o Alexa utilizan IA para realizar tareas como responder preguntas y controlar dispositivos del hogar inteligente. Uber emplea IA para asignar conductores, calcular tiempos estimados de llegada y optimizar rutas. Plataformas como Netflix o Spotify utilizan IA para recomendar contenido basado en las preferencias del usuario. Además, modelos de IA generativa como ChatGPT están revolucionando áreas como el servicio al cliente, la educación, y el entorno laboral, respecto del que se recomienda verificar la información obtenida *fact-check*. En el ámbito legal, herramientas como Harvey, en uso en Perú, o Maite.ai y otros, permiten analizar grandes cantidades de documentos legales y generar borradores de contratos, así como absolver consultas legales, entre otros.

La IA ha evolucionado significativamente desde sus inicios, avanzando desde sistemas expertos básicos hasta modelos sofisticados de aprendizaje profundo y generativo. Su impacto es evidente en la vida cotidiana, desde asistentes virtuales hasta aplicaciones avanzadas en el ámbito legal, comercial y otros. La IA generativa, en particular, ha demostrado su capacidad para crear contenido similar al humano, mostrando su potencial para transformar múltiples sectores. A continuación, veremos la incidencia que tiene en el ámbito laboral y sus innegables beneficios al igual que los desafíos que plantea.

II. LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO LABORAL: RIESGOS Y OPORTUNIDADES

La IA está transformando el lugar de trabajo al automatizar tareas rutinarias como cognitivas, lo que incrementa la eficiencia y productividad. Su uso

abarca desde la selección de personal hasta la gestión y monitoreo de empleados e incluso la extinción del vínculo laboral. Sin embargo, esta adopción acelerada trae consigo riesgos significativos como la perpetuación de sesgos, la invasión de la privacidad y el impacto en la salud mental de los trabajadores.

Una diferencia significativa entre la IA y tecnologías anteriores es su capacidad para automatizar tareas no rutinarias que requieren habilidades cognitivas avanzadas como el razonamiento deductivo y la ordenación de información. Aunque la IA mejora muchos aspectos del trabajo, también puede intensificar la carga laboral y aumentar el estrés. Su implementación puede afectar la privacidad y autonomía de los trabajadores, y amplificar sesgos existentes, lo que podría impactar desproporcionadamente a grupos desfavorecidos (OCDE, 2023, p. 98).

La rápida adopción de la IA afecta a múltiples sectores. A pesar de sus beneficios, como la mejora en la toma de decisiones y el aumento de la productividad, la IA también puede desplazar empleos altamente calificados y aumentar la desigualdad si no se garantiza un acceso equitativo a esta tecnología (OCDE, 2024). Se estima que la IA afectará aproximadamente el 40% de los empleos a nivel mundial, reemplazando algunos y complementando otros. Si bien puede revitalizar la productividad y estimular el crecimiento, también podría profundizar la desigualdad, especialmente en economías emergentes con infraestructuras inadecuadas y fuerzas laborales menos cualificadas (Cazzaniga y otros, 2024).

Como vemos el impacto de la IA en términos de productividad y eficiencia es positiva. Procesa grandes volúmenes de información que se potencia aún más una vez integrado a un ecosistema digital aplicado al trabajo. No obstante ello, también trae consigo claros desafíos que como veremos a continuación afectan la privacidad, pueden generar discriminación y generan riesgos psicosociales. Estos riesgos están siendo abordados por las distintas legislaciones de la IA para mitigarlos a partir de principios rectores como minimización de datos personales, explicabilidad, supervisión humana y transparencia.

1. Gestión y vigilancia de los trabajadores con IA

La implementación de IA ha introducido un nuevo nivel de vigilancia laboral, utilizando datos como la gestión del tiempo, pulsaciones de teclas, interacciones en redes sociales, registros de llamadas, capturas de pantalla, consultas de búsqueda, seguimiento ocular, software de reconocimiento facial, sensores

en teléfonos y gafas inteligentes, entre otros. Una característica neurálgica de la IA es su capacidad para integrarse con prácticas ya existentes, permitiendo una recopilación masiva de datos detallados sobre el comportamiento de los trabajadores. Indicadores simples, como la cantidad de correos electrónicos enviados, los sitios web visitados, las cookies, y los documentos abiertos, se usan para tomar decisiones de gestión aparentemente basadas en datos de trabajo. Estas prácticas permiten una recopilación masiva de información detallada sobre los trabajadores, que luego se utiliza para tomar decisiones de gestión basadas en datos (Aloisi & Gramano, 2019).

Por ejemplo, en Amazon Italia, los algoritmos gestionan las tareas y supervisan a los trabajadores en sus almacenes, automatizando funciones de gestión y reduciendo la necesidad de supervisores humanos (Delfanti, 2019).

La gestión algorítmica, un conjunto de herramientas tecnológicas utilizadas para administrar la fuerza laboral de forma remota mediante la recopilación de datos y la vigilancia, permite la toma de decisiones automatizada o semi-automatizada. Esta tecnología ejecuta funciones de dirección y supervisión con o sin intervención humana. Genera la reestructuración de cadenas de suministro como los modelos de producción *just in time* de Walmart o Zara, se establecen jornadas y horarios sobre la base de la demanda o concurrencia de clientes a centros de trabajo, y se utilizan cada vez más en la contratación para tomar decisiones y filtrar currículums, así como se integra en la infraestructura laboral para expandir la vigilancia y recopilación de datos (Mateescu & Nguyen, 2019).

La toma de decisiones automatizadas y la vigilancia constante a través de dispositivos portátiles e internet de las cosas pueden generar estrés y riesgos psicosociales, debido a la falta de privacidad. En los *call centers*, los algoritmos vigilan detalladamente las llamadas y evalúan la empatía y cortesía de los trabajadores, creando rankings que pueden afectar su evaluación laboral (Todolí, 2019, 2022). Expertos advierten que esta automatización puede perpetuar sesgos discriminatorios y socavar la justicia en el entorno laboral, alterando el equilibrio de poder y promoviendo una cultura de medición individual y auto-seguimiento (Aloisi & Gramano, 2019).

En 2014 Amazon desarrolló una herramienta de reclutamiento basada en IA que generó discriminación por género. La compañía descubrió en 2015 que su sistema no evaluaba a los candidatos de manera neutral en cuanto al género. Los modelos de IA, que habían aprendido de currículums de trabajadores pre-

dominantemente masculinos de los últimos 10 años, tendían a favorecer a los candidatos masculinos. Por ejemplo, penalizaban los currículums que incluían términos como “club de ajedrez femenino” y disminuían puntaje a graduadas de universidades exclusivamente femeninas. Ello ilustra los peligros de implementar IA sin supervisión adecuada (Dastin, 2018). En contraste, la plataforma de reclutamiento ecuatoriana Evaluar³, entre otras, con presencia en Perú, adopta un enfoque ético y transparente, asegurando que los candidatos no sean evaluados exclusivamente por decisiones automatizadas y ofreciendo mecanismos para impugnar decisiones basadas en IA, destacando la importancia de salvaguardas éticas y legales en su uso.

La IA ha transformado la forma de dirección y supervisión del empleador sobre el trabajador, así como la evaluación y toma de decisiones en el entorno laboral sustentado en los macrodatos del desempeño y comportamiento del trabajador, ya sea para determinar su capacidad, otorgar bonificaciones, ascensos, imponer sanciones disciplinarias o extinguir el vínculo laboral. Estos aspectos plantean riesgos significativos, como la perpetuación de sesgos, invasión de la privacidad y el aumento de riesgos psicosociales, los que, en conjunto con diversos elementos, son considerados por la legislación comparada para regular el uso de la IA en el entorno laboral como veremos a continuación.

2. Regulación y protección de derechos laborales ante la IA

a) Regulación comparada sobre la IA y efectos en el ámbito laboral

En las regulaciones que mencionaremos, se adoptan como principios rectores la transparencia, explicabilidad, supervisión humana y minimización del uso de datos personales. Estos principios son esenciales para garantizar que los sistemas de IA durante todo su ciclo de vida se desarrollen y apliquen de manera responsable, protegiendo los derechos fundamentales y evitando riesgos significativos en ámbitos como el laboral, donde la vigilancia y la toma de decisiones automatizadas pueden tener un impacto profundo en la privacidad, la discriminación y el bienestar de los trabajadores.

3 De acuerdo con su Política de Protección de Privacidad y Protección de Datos la plataforma asegura el derecho de los candidatos a no ser evaluados exclusivamente por decisiones automatizadas. EVALUAR. Política de Protección de Datos. Recuperado de <https://www.evaluar.com/politica-de-proteccion-de-datos-evaluar-v1>

La OCDE adoptó como instrumento jurídico la Recomendación del Consejo sobre Inteligencia Artificial el 21 de mayo de 2019, modificada en 2023 y 2024. Esta recomendación toma en cuenta varios marcos internacionales y normativos, incluyendo las normas de la OCDE, los Objetivos de Desarrollo Sostenible de la Agenda 2030 y la Declaración Universal de Derechos Humanos. La recomendación cuenta con dos secciones principales, i) principios para la gestión responsable de una IA fiable y ii) políticas nacionales y cooperación internacional para una IA confiable. Con relación a la primera establece como principios, entre otros:

- i. Respeto del estado de derecho y derechos humanos: Garantizar la no discriminación, la privacidad y los derechos laborales durante todo el ciclo de vida de la IA.
- ii. Transparencia y explicabilidad: Divulgar información clara sobre los sistemas de IA, permitiendo a los afectados comprender y cuestionar los resultados.
- iii. Responsabilidad: Establecer la trazabilidad y la gestión de riesgos para garantizar el correcto funcionamiento y la responsabilidad en los sistemas de IA.

La recomendación destaca la necesidad de equilibrar la innovación con la protección de derechos fundamentales y promover políticas que apoyen una IA confiable y ética. Perú se ha adherido a esta recomendación lo que la constituye como normativa *soft law*. En esa línea, la Recomendación sobre la Ética de la IA adoptada el 23 de noviembre de 2021 de la UNESCO, establece un marco de valores y principios éticos destinados a guiar el desarrollo y la implementación de sistemas de IA. A continuación, se resumen parte de los principios que adopta:

- i. Proporcionalidad e inocuidad: Los sistemas de IA deben ser proporcionales y adecuados al contexto en el que se utilizan, evitando cualquier daño innecesario a seres humanos, comunidades o al medio ambiente.
- ii. Equidad y no discriminación: Los sistemas de IA deben promover la justicia social y evitar cualquier forma de discriminación, asegurando que los beneficios de estas tecnologías estén disponibles para todos.
- iii. Derecho a la intimidad y protección de datos: La privacidad de los individuos debe ser respetada y protegida, garantizando que los datos

utilizados en los sistemas de IA se gestionen de manera coherente con los marcos legales pertinentes.

- iv. Supervisión y decisión humanas: Las decisiones importantes que involucren sistemas de IA deben estar bajo la supervisión humana, asegurando que la responsabilidad final recae en los seres humanos.
- v. Transparencia y explicabilidad: Los sistemas de IA deben ser transparentes y explicables, permitiendo a los usuarios comprender cómo se toman las decisiones.

En esa línea, el RIAUE al igual que las directrices de la OCDE y la UNESCO, enfatiza la importancia de la supervisión humana, la transparencia y la explicabilidad en el uso de sistemas de IA, tal como se establece en el artículo 14 de este reglamento. En efecto, exige que los sistemas de IA sean transparentes y explicables, permitiendo a los usuarios y personas afectadas entender cómo se toman las decisiones mediante IA y asegurando que se informen de manera adecuada, proporcionando información clara sobre su funcionamiento, los datos utilizados y la toma de decisiones, como se detalla en sus artículos 11 y 12.

Además, el RIAUE clasifica la IA según los riesgos y establece una serie de prohibiciones y obligaciones en función de cada uno de ellos (UE, 2024):

- I. Riesgo inaceptable: Incluye sistemas de IA que representan una amenaza para las personas, como la manipulación cognitiva de personas vulnerables, la puntuación social y el reconocimiento facial en tiempo real. Estos sistemas están prohibidos, con excepciones como la identificación biométrica a distancia “a posteriori” para perseguir delitos graves con aprobación judicial.
- II. Riesgo alto: Se refiere a sistemas de IA que afectan la seguridad, salud o derechos fundamentales, incluyendo el ámbito laboral en la gestión de trabajadores, la identificación biométrica y la categorización de personas físicas.

El considerando 53 del RIAUE indica que algunos sistemas de IA que realizan tareas limitadas, como la estructuración de datos o la traducción de documentos, no representan un riesgo significativo y deben ser documentados como de bajo riesgo. En contraste, el considerando 57 clasifica los sistemas de IA en el ámbito laboral como de alto riesgo debido a su impacto potencial en los derechos y perspectivas laborales, ya que pueden perpetuar discriminaciones y vulnerar la privacidad y protección de datos personales.

En relación con el ámbito laboral, el RIAUE considera como prácticas prohibidas en el artículo 5 el uso de sistemas de IA para inferir emociones en los lugares de trabajo, excepto cuando se trate de motivos médicos o de seguridad. También prohíbe el uso de sistemas de categorización biométrica que clasifiquen a personas físicas para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas, vida u orientación sexuales. Respecto a sistemas de IA de alto riesgo, el artículo 6 y Anexo III, del RIAUE incluye sistemas de identificación biométrica remota, categorización biométrica y reconocimiento de emociones. En específico sobre el ámbito laboral, clasifica como de alto riesgo a los sistemas de IA utilizados para la contratación, selección de personal, evaluación de candidatos, toma de decisiones sobre relaciones laborales, asignación de tareas, y supervisión del rendimiento y comportamiento de los trabajadores.

El Artículo 9 del RIAUE exige que los sistemas de IA de alto riesgo cuenten con un sistema de gestión de riesgos continuo y actualizado, que identifique y mitigue riesgos para la salud, seguridad y derechos fundamentales. Este sistema debe ser probado antes de su uso para asegurar su eficacia y minimizar riesgos, especialmente en entornos laborales y para grupos vulnerables. El artículo 14 establece que los sistemas de IA de alto riesgo deben diseñarse para permitir una supervisión humana efectiva mediante interfaces adecuadas. La supervisión busca minimizar riesgos para la salud, seguridad o derechos fundamentales, tanto en el uso previsto como en el mal uso razonablemente previsible, incluso cuando persisten riesgos tras aplicar otros requisitos.

El profesor Sanguineti (2024, pp. 5-6) sostiene que estas disposiciones favorecen el uso de la IA con pleno respeto a los derechos fundamentales laborales, prohibiendo sistemas de IA que representan riesgos intolerables, como la categorización biométrica y la detección de emociones en el trabajo. También destaca la importancia de implementar sistemas de gestión de riesgos en sistemas de alto riesgo relacionados con la contratación, gestión y evaluación de trabajadores. Por su parte, Menor (2024) considera respecto a esta regulación que los empleadores que utilicen IA en la contratación, evaluación y gestión de empleados deben cumplir con estrictas protecciones, que incluyen la supervisión humana, validación de datos, monitoreo de sistemas y evaluación del impacto sobre los derechos fundamentales.

Igualmente, se ha previsto en el artículo 22 del Reglamento General de Protección de Datos de la Unión Europea el derecho de las personas a no ser

sometidas a decisiones basadas únicamente en el procesamiento automatizado de sus datos si estas decisiones tienen implicaciones legales o afectaciones significativas. Esto es supervisión humana. También obliga a las empresas a informar a los trabajadores sobre la lógica empleada en decisiones automatizadas y su impacto. Notas características del principio de explicabilidad.

Por su parte el artículo 64.4 d) del Estatuto de los Trabajadores español exige que se informe a los representantes legales de los trabajadores y sindicatos sobre los parámetros, reglas e instrucciones de los algoritmos o sistemas de IA que puedan impactar en las condiciones de trabajo y empleo. También vemos la presencia del principio de explicabilidad en estas disposiciones.

A mayor abundamiento, la orden ejecutiva emitida por el presidente Joe Biden el 30 de octubre de 2023 *“Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”*, abarca una amplia gama de principios y políticas para regular el desarrollo y uso de la IA en los Estados Unidos de América. Incluyendo entre ellas supervisión humana, explicabilidad, transparencia, el apoyo a trabajadores, equidad, datos personales, privacidad y libertades civiles. El propósito de la orden es maximizar los beneficios de la IA, al tiempo que se mitigan sus riesgos significativos, que incluyen fraudes, discriminación, desplazamiento laboral, y amenazas a su seguridad nacional.

La Tabla 1 muestra un comparativo sobre la diversa regulación y propuestas legales de IA de diversos países, entre ellos Argentina, Brasil, Chile y otros, considerando los principales aspectos que regulan o buscan normar. Esto es si realizan una clasificación de riesgo de IA tal como el RIAUE, si contienen disposiciones específicas en el ámbito laboral, así como si recogen principios de explicabilidad, transparencia, supervisión humana, privacidad y datos personales.

Tabla 1
Sobre la regulación de la IA

Pais/Estado/Ciudad	Regulación/Propuesta	Principales aspectos	Categorización de riesgo de la IA	Contratación, gestión y terminación de relación laboral	Principios regulados
Argentina	Disposición N° 2/2023 y Comunicación A 7724 del BCRA	Recomendaciones para IA fiable, requisitos mínimos para la gestión de riesgos tecnológicos y de seguridad de la información.	No especifica	Enfocado principalmente en la seguridad de la información y gestión de riesgos tecnológicos, no directamente en la contratación y	Supervisión humana, explicabilidad, datos personales, transparencia
Brasil	Proyecto de Ley 2338/2023	Protección de datos personales, derechos de los titulares de datos, sanciones por incumplimiento, gobernanza de datos, desarrollo e implementación de IA basada en principios éticos y derechos humanos, responsabilidad civil, sandbox regulatorio.	Sí, sistemas de alto riesgo y riesgo excesivo	Regula el uso de IA en el contexto laboral, incluyendo contratación, gestión de empleados y evaluación de desempeño.	Supervisión humana, transparencia, explicabilidad, datos personales
Chile	Proyecto de Ley sobre robótica, inteligencia artificial y tecnologías conexas	Clasificación de sistemas de riesgo, protección de datos personales, no discriminación algorítmica, responsabilidad civil, derechos de propiedad intelectual.	Sí, sistemas de riesgo inaceptable y alto riesgo	Regula el uso de IA en la contratación y evaluación de empleados, asegurando transparencia y equidad.	Supervisión humana, explicabilidad, transparencia, datos personales
California (EE.UU.)	Proyecto de Ley AB331 sobre herramientas de decisión automatizada	Normas sobre uso de herramientas de decisión automatizada, transparencia, equidad, protección de datos personales.	No especifica	Se enfoca en la equidad y transparencia en el uso de herramientas automatizadas para la contratación y evaluación de empleados.	Decisiones de consecuencias significativas, evaluación de impacto
China	Medidas Administrativas para los servicios de IA Generativa	Control de servicios de IA generativa, estándares de seguridad, protección de datos, supervisión estatal.	No especifica	No especifica directamente, pero incluye controles que pueden afectar el uso de IA en la gestión de empleados.	Supervisión humana, transparencia, explicabilidad, datos personales
Nueva York (EE.UU.)	Ley 144/2021 sobre IA en contratación de personal	Uso de IA en procesos de contratación, transparencia, equidad, no discriminación, derechos de los candidatos.	No especifica	Específicamente dirigida a la contratación, garantizando la equidad y transparencia en el uso de IA para evaluar candidatos.	Transparencia, explicabilidad, no discriminación, equidad en la contratación
Reino Unido	Enfoque favorable a la innovación para la regulación de IA	Fomento de la innovación, desarrollo de estrategias nacionales de IA, principios y recomendaciones para la aplicación de IA.	No especifica	Incluye principios que promueven la equidad y transparencia en el uso de IA en el empleo y la gestión de trabajadores.	Seguridad, transparencia, explicabilidad, equidad, rendición de cuentas, contestabilidad y compensación
Japón	Libro Blanco de IA	Promoción de la investigación y desarrollo, acumulación y coordinación de datos, uso activo de IA en servicios públicos, apoyo a ciudades inteligentes.	No especifica	Enfocado en la promoción de IA en servicios públicos, no directamente en la contratación y gestión de empleados.	Supervisión Humana, transparencia, innovación responsable y seguridad

Nota. Adaptado de “Propuestas de regulación y recomendaciones de inteligencia artificial en el mundo” por Corvalán, Sánchez Caparrós, Raban, Stringhini, Papini, Heleg y Bonato, (2023). Pontificia Universidad Católica de Argentina. Recuperado de https://www.researchgate.net/publication/372215967_Propuestas_de_regulacion_y_recomendaciones_de_inteligencia_artificial_en_el_mundo. Información de dominio público.

Como hemos visto, la regulación está evolucionando para abordar los desafíos que la IA presenta, en específico su uso en el ámbito laboral. Las disposiciones y propuestas revisadas reflejan un compromiso y tendencia global para asegurar que la implementación de IA sea ética, transparente y protectora de los derechos humanos y en particular de los derechos laborales. Más allá de la técnica legislativa por la que se haya optado para su regulación, bien sea insuficiente o pueda calificarse de excesiva al prohibir o permitir su uso con determinadas condiciones en función a la perspectiva con la que se analice, lo que podemos observar es que todas ellas tienen como denominador común principios o disposiciones sobre transparencia, explicabilidad, minimización de datos personales, no discriminación, privacidad y supervisión humana que apuntalan el uso ético y productivo de la IA en el entorno laboral.

b) La regulación laboral y constitucional en Perú y la aplicación de sistemas de IA: Facultades del empleador y límites basados en los derechos fundamentales, protección de datos personales y el principio de proporcionalidad

La Ley 31814, que promueve el uso de la IA en Perú, más allá de esbozar definiciones, no realiza regulación alguna sobre el uso de la IA. El Proyecto

de Reglamento de esta ley (PRLIA), aprobado por Resolución Ministerial N° 132-2024-PCM, establece principios rectores como la protección de la dignidad humana y datos personales, no discriminación, privacidad, ética, transparencia, sostenibilidad, replicabilidad, responsabilidad y supervisión humana. Estos principios se alinean con los estándares internacionales que hemos visto en el punto anterior. Asimismo, el PRLIA sigue la regulación del RIAUE, puesto que clasifica los riesgos de los sistemas de IA según su impacto en el trato equitativo, transparencia y derechos fundamentales. Se prohíben los sistemas de riesgo inaceptable, como aquellos que explotan vulnerabilidades o clasifican a personas de manera perjudicial y desproporcionada. Para los sistemas de alto riesgo, como los utilizados en la gestión laboral automatizada como selección, contratación o terminación de la relación laboral, se establecen obligaciones específicas, incluyendo la necesidad de supervisión humana, evaluación de riesgos y la implementación de medidas de seguridad desde su diseño.

Como se podrá notar Perú no cuenta con una regulación específica sobre la IA, igualmente en el ámbito laboral; no obstante, la regulación laboral⁴ y constitucional, la normativa sobre protección de datos personales, así como la jurisprudencia sobre la materia constituyen un sistema de garantías mínimo de protección del trabajador frente a la implementación de sistemas de IA por parte del empleador en el entorno laboral.

La Constitución Política del Perú (CPP) en su artículo 59, consagra la libertad de empresa, la cual incluye la facultad de organización y dirección de la actividad empresarial de acuerdo con los recursos disponibles y las condiciones del mercado. Este marco constitucional otorga al empleador un poder significativo para estructurar y gestionar su organización con el objetivo de maximizar la eficiencia y competitividad (caso 1405-2010-AA/TC, f. 15). La Ley de Productividad y Competitividad Laboral (TUO del D.L. 728, aprobado por D.S. 003-97-TR) en su artículo 9 refuerza esta potestad, otorgando al empleador la

4 Véase por ejemplo, la Ley N° 31572 de Teletrabajo y su Reglamento (D.S N° 002-2023-TR) protegen el derecho de las personas teletrabajadoras a la intimidad, privacidad e inviolabilidad de sus comunicaciones y documentos privados. El Artículo 6.4 de la Ley establece este derecho, mientras que el Artículo 9 del Reglamento detalla que los empleadores deben respetar estos derechos al implementar medios de control y supervisión en el teletrabajo. Específicamente, el reglamento prohíbe acceder a documentos y comunicaciones sin autorización, realizar grabaciones de imagen o voz sin consentimiento, excepto cuando sea necesario por la naturaleza de sus funciones, ingresar al lugar de teletrabajo sin permiso, y utilizar mecanismos que vulneren la intimidad del teletrabajador.

facultad de dirigir, fiscalizar y sancionar a sus trabajadores, siempre dentro de los límites de la razonabilidad y teniendo en cuenta las necesidades del centro de trabajo.

El ejercicio de estas facultades no puede—y no debe—vulnerar los derechos constitucionales de los trabajadores. El artículo 23 de la CPP es claro en que ninguna relación laboral puede limitar el ejercicio de los derechos fundamentales ni afectar la dignidad del trabajador (caso 1058-2004-AA/TC, f.19). Este paradigma es esencial para cualquier política o práctica laboral, incluyendo aquellas que implican la implementación de sistemas de IA.

En esa línea, la jurisprudencia del Tribunal Constitucional⁵ (TC) ha sido fundamental al definir el contenido esencial de los derechos laborales, interpretar sus alcances y expulsar del ordenamiento jurídico normas por inconstitucionales con la finalidad de proteger los derechos fundamentales del trabajador (Sanguinetti, 2008, p. 76), el que actualmente continúa incidiendo en esa línea.

Así su intervención para otorgar prevalencia a los derechos constitucionales del trabajador dentro de la relación de trabajo, derechos inespecíficos, frente a las facultades del empleador basado en el principio de proporcionalidad tal como ha sido desarrollado por la jurisprudencia del TC requiere que cualquier medida empresarial cumpla con criterios de idoneidad, necesidad y proporcionalidad en sentido estricto. Esto implica que la medida debe ser adecuada para el objetivo empresarial, la menos restrictiva posible, y equilibrar adecuadamente los derechos del trabajador con el beneficio obtenido⁶. En la Casación Laboral N.º 09636-2019-LIMA, la Corte Suprema, siguiendo estos criterios, determinó que realizar pruebas de detección de alcohol y drogas en viviendas de trabajadores en unidades mineras no era proporcional, ya que vulneraba el derecho a la inviolabilidad del domicilio. Mientras que en el caso N.º 2208-2017-PA/TC, el TC respaldó la instalación de cámaras de videovigilancia en áreas de trabajo para la supervisión e incluso sanción de empleados al no verificarse la vulneración al derecho fundamental de intimidad de aquellos, puesto que tuvo por finalidad asegurar la seguridad de los trabajadores y la correcta ejecución de sus labores.

5 Decisiones como en el Exp. 1058-2004-AA/TC sobre privacidad, el Exp. 4635-2004-AA/TC sobre igualdad laboral, y el Exp. 0895-2001-AA/TC sobre libertad de religión en el trabajo, destacan por su papel en la protección de derechos fundamentales en el ámbito laboral.

6 El TC ha aplicado este principio en sentencias como los casos 2250-2007-PA/TC y 535-2009-PA/TC, evaluando la razonabilidad y proporcionalidad de sanciones disciplinarias.

En esa orden de ideas, como parte del sistema de garantías mínimo, las disposiciones de protección de datos personales que como derecho constitucional se encuentra consagrado en el artículo 2, numeral 6, de la CPP, garantiza a toda persona el control sobre su información personal, evitando su divulgación indebida. El derecho a la autodeterminación informativa permite a los individuos controlar cómo se registran, usan y difunden sus datos, un derecho delineado por el TC en el caso N° 04739-2007-PHD/TC.

Su desarrollo legislativo se encuentra en la Ley N° 29733, Ley de Protección de Datos Personales (LPDP) y su reglamento. La LPDP establece como rectores al principio consentimiento, de finalidad y proporcionalidad en sus artículos 5, 6 y 7, respectivamente. El primero dispone que para el tratamiento de los datos personales debe mediar el consentimiento de su titular; el segundo, que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita, y no deben ser tratados para otros fines sin el consentimiento informado del titular. El tercero, exige que el tratamiento de datos personales sea adecuado, relevante y no excesivo respecto a la finalidad para la cual han sido recopilados. La LPDP define los datos personales como cualquier información que identifica o hace identificable a una persona, y distingue los datos sensibles, que incluyen información sobre salud, vida sexual, origen racial, afiliación sindical, entre otros, los cuales requieren un consentimiento explícito y escrito para su tratamiento. Su Reglamento añade que los datos sensibles comprenden información sobre características físicas, emocionales, vida afectiva, y cualquier otra información que afecte la intimidad de la persona.

Existen excepciones al consentimiento del titular de los datos personales previstos en el artículo 14 de LPDP, tal como “para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte”, supuesto en el que se subsume la relación laboral. Los datos personales del trabajador serán tratados sin su consentimiento si son necesarios para la ejecución de la relación laboral. Para realizar este tratamiento se debe observar el principio de finalidad y proporcionalidad, así como el derecho a ser informado en “forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados” conforme al artículo 18 de la LPDP y su reglamento. Ello delimita los alcances de su tratamiento y permitirá el ejercicio del derecho de oposición por parte del trabajador en caso de exceder la finalidad para el que fueron recopilados sus datos.

Sobre estos mismos principios se delinea la Directiva N° 01-2020-JUS/DGTAIPD, que regula el uso de sistemas de videovigilancia en el ámbito laboral, permitiendo su implementación sin el consentimiento de los trabajadores, siempre que se respete el principio de proporcionalidad y se informe previamente a los empleados sobre la finalidad de su tratamiento mediante carteles informativos u otros medios. Esto incluye restricciones sobre la instalación de cámaras en espacios de descanso y la captación de sonido, salvo que existan riesgos relevantes para la seguridad de las instalaciones, bienes y personas. Del mismo modo, la Opinión Consultiva N° 045-2021-JUS/DGTAIPD de la autoridad de datos personales del país reitera que el empleador debe evaluar la proporcionalidad del uso de videovigilancia para el control laboral caso por caso. Específicamente, se considera proporcional cuando se requiere cumplir con medidas de seguridad en trabajos de riesgo, como verificar el uso de implementos de seguridad o el uso correcto de máquinas.

Otras opiniones consultivas han legitimado el tratamiento de datos sensibles sin consentimiento del trabajador, como en el caso del control de asistencia mediante huella digital (Oficio N° 862-2016-JUS/DGPDP) o la detección de COVID-19, debiendo estar vinculado a la seguridad y salud laboral de acuerdo a la Opinión Consultiva N° 32-2020-JUS/DGTAIPD que consideró legítimo medir la temperatura corporal de los trabajadores para prevenir la propagación del virus en cumpliendo de las obligaciones de prevención en materia de seguridad y salud en el trabajo por parte del empleador. En ambos casos, se precisó que el empleador se encuentra obligado a observar el deber de informar al trabajador conforme al artículo 18 de la LPDP.

La normativa peruana sobre protección de datos personales en el marco de la relación laboral impone obligaciones a los empleadores, garantizando que el tratamiento de datos personales y sensibles de los trabajadores cumpla con los principios rectores de finalidad y proporcionalidad, así como con el respeto a su derecho de información.

Como vemos el ordenamiento jurídico revisado constituye un sistema de protección mínimo del trabajador frente al uso de la IA en el entorno laboral, fundamentado en la normativa laboral, los derechos inespecíficos reconocidos por la CPP al interior de la relación laboral, la regulación de protección de datos personales, así como por la jurisprudencia del TC. En este contexto, el uso de la IA por parte de los empleadores en la gestión y control laboral debe estar

estrictamente delimitado por criterios de proporcionalidad y razonabilidad. En efecto, es imprescindible que cualquier uso de IA esté precedido por un riguroso análisis para garantizar que las medidas adoptadas sean las menos intrusivas y las más adecuadas para cumplir con los objetivos empresariales, sin comprometer los derechos de los trabajadores. La implementación de estas tecnologías requiere una finalidad clara y legítima, comunicada adecuadamente al trabajador, y debe respetar plenamente sus derechos fundamentales. El empleo de sistemas de IA en el entorno laboral, ya sea para la selección, evaluación, gestión, supervisión o terminación del contrato, debe ir acompañado de una obligación ineludible de transparencia e información por parte del empleador.

Por ello, dotar de mayor contenido y alcance al derecho de información en el ámbito laboral previsto en la regulación de datos personales constituiría un componente relevante para fortalecer las garantías mínimas del sistema jurídico de protección del trabajador frente al uso de la IA en el ámbito laboral. Esto es transparencia al aplicarla asegurando se cumpla con el principio de explicabilidad. El diccionario de la Real Academia Española define transparente como claro, evidente, que se comprende sin duda ni ambigüedad. También como una gestión o proceso que se realiza sin que se oculte información sobre la manera en que se hace o se desarrolla. A partir de ello la aplicación de sistemas de IA en el ámbito laboral deberían ir acompañadas con una explicación clara y sencilla sobre su finalidad y funcionamiento a los trabajadores, que implica dar a conocer los parámetros, reglas e instrucciones de los sistemas de IA a utilizar que generen impacto en el proceso de selección o durante la relación de trabajo.

Ello es necesario puesto que la normativa laboral vigente, de datos personales y jurisprudencia no exige que los empleadores expliquen a los trabajadores cómo funcionan los sistemas de IA, ni que aseguren la supervisión humana en decisiones automatizadas sustanciales y significativas que impacten en el trabajador o la minimización de datos en su tratamiento que implica que solo se recopilen y almacenen los datos estrictamente necesarios para cada propósito establecido de forma temporal, asegurando que sean adecuados y no excedan lo requerido para dicho fin. Estos aspectos podrían abordarse mediante mecanismos de autorregulación regulada (*compliance*) del empleador, asegurando así un respeto pleno a los derechos de los trabajadores en el uso ético de la IA para que sea fiable en el ámbito laboral.

Alinearse con los estándares internacionales de regulación en materia laboral que recogen los principios que hemos señalado en relación con la aplicación de la IA, consolidaría un marco regulatorio robusto que no solo protege los derechos de los trabajadores, sino que también fomenta un entorno empresarial competitivo y sostenible, capaz de aprovechar las ventajas de la IA para mejorar la productividad y competitividad con pleno respeto a los derechos de privacidad y no discriminación de los trabajadores.

El derecho laboral actúa como un contrapeso esencial frente al poder empresarial, especialmente en un contexto de cambios organizacionales impulsados por la tecnología. La IA, aunque presenta oportunidades para mejorar la eficiencia y productividad, también trae consigo el riesgo de amplificar las desigualdades estructurales y erosionar los derechos fundamentales si no se regula adecuadamente.

El derecho laboral tiene una función integradora en el conflicto estructural inherente a la relación de trabajo asalariado, equilibrando la libertad empresarial y los poderes del empleador con la protección del trabajador, compensando las desigualdades de la parte más débil. Este equilibrio es especialmente necesario en el contexto de los cambios organizacionales derivados de la tecnología, la globalización y la descentralización que requiere adaptar las normas laborales para abordar las nuevas formas de organización del trabajo contemporáneo (Palomeque, 2011, pp. 37-39, 46).

La implementación de la IA en el entorno laboral debería ir más allá del cumplimiento normativo, adoptando políticas internas que aseguren un uso ético y transparente. Es determinante que los empleadores informen a los trabajadores sobre la lógica de las decisiones automatizadas, garanticen la explicabilidad, mitiguen riesgos e integren la supervisión humana para prevenir sesgos, todo bajo el principio de proporcionalidad y finalidad de tratamiento de datos personales. Este enfoque no solo protege los derechos de los trabajadores, sino que también alinea las prácticas laborales con los estándares más altos en protección de datos y justicia laboral. Estas prácticas podrían mitigar el riesgo de percepción de invasión de privacidad y riesgos psicosociales, al permitir que los trabajadores comprendan el uso, procesamiento y decisiones automatizadas o semiautomatizadas basadas en sistemas de IA.

c) **Aplicación de sistemas de IA para optimizar la seguridad y salud en el trabajo**

La implementación de sistemas de IA para la mejora continua del sistema de gestión de Seguridad y Salud en el Trabajo (SST) aprovechando su capacidad para monitorear y analizar datos en tiempo real permite la detección precoz de riesgos y el uso de análisis predictivo para prevenir accidentes, reduciendo la incidencia de accidentes y enfermedades laborales mediante alertas tempranas y datos precisos. Un ejemplo concreto es la analítica de cámaras de video vigilancia con IA que disminuye los accidentes en materia de SST. Sin embargo, la vigilancia intensiva mediante macrodatos puede afectar negativamente la salud mental de trabajadores debido a la percepción de vigilancia constante (Macias, 2023).

Por ello, el empleador como garante de la SST, debe evaluar cuidadosamente si estas prácticas contribuyen al cumplimiento de sus obligaciones legales en materia de SST y se alinea al sistema jurídico de garantía mínimo de protección del trabajador frente a la implementación de IA en el ámbito laboral, además de observar los principios que hemos mencionado como parte de su regulación interna. Para que su aplicación tenga un impacto positivo, es ineludible identificar cuándo y dónde utilizar estas herramientas, lo que implica automatizar procesos mecánicos y manuales para enfocarse en tareas críticas.

Por ejemplo, en Perú, empresas como Safetymind IA han implementado analítica de cámaras de videovigilancia basadas en IA para mejorar la SST en sectores como minería, siderurgia y transporte. Estas tecnologías, aplicadas a la medida de las necesidades de cada sector, no requieren una inversión significativa, ya que el software de analítica puede aplicarse a cámaras existentes, permitiendo detectar aspectos críticos en SST y generar alertas visuales o sonoras, o incluso deteniendo maquinaria de manera preventiva. Este tipo de vigilancia continua reemplaza y/o potencia las inspecciones diarias, automatizando la recolección de datos las 24 horas del día, los 7 días de la semana.

Estos sistemas de IA pueden identificar personas que ingresan a zonas restringidas mediante reconocimiento facial, si están demasiado cerca de maquinaria pesada, o conductores que no mantienen las manos en el volante durante más de 20 segundos o estén con somnolencia. También pueden detectar si los trabajadores están utilizando Equipos de Protección Personal (EPPs) adecuados durante actividades de alto riesgo, emitiendo alertas en tiempo real a los trabajadores. También, delimitan áreas de trabajo y detectan su traspaso para alertar

a los trabajadores. Este modelo de IA se autocorrigue con el tiempo para ser más eficaz, alcanzando hasta un 98% de precisión (Acuña, 2024).

Igualmente, si un vehículo pesado traspasa la distancia mínima de seguridad, las cámaras de videovigilancia con analítica envían una alerta inmediata al conductor para detener el trabajo y prevenir un accidente. Este sistema no solo detecta conductas subestándar, sino que emite alertas preventivas que pueden evitar accidentes graves.

La incorporación de sistemas de IA de analítica de imágenes y videos de cámaras de videovigilancia fortalece significativamente el cumplimiento de las obligaciones del empleador en materia de SST previstas en la Ley N° 29783 (LSST) y su Reglamento (Decreto Supremo N° 05-2012-TR) y demás disposiciones. Estos sistemas permiten un monitoreo continuo y una evaluación constante de riesgos a partir de la analítica de datos recopilados por las cámaras, facilitando la actualización del IPERC (Identificación de Peligros, Evaluación de Riesgos y Determinación de Controles) con datos precisos y actuales, mejorando así la seguridad laboral para fortalecer los controles continuamente.

El principio de prevención exige que el empleador garantice medios que protejan la vida y salud de los trabajadores, mientras que el principio de protección asegura condiciones de trabajo dignas y seguras. El principio de responsabilidad establece que el empleador asume las consecuencias de accidentes o enfermedades laborales, todos previstos en el Título Preliminar de la LSST. Los artículos 20, 21 y 49 de la LSST y el artículo 77 del RLSST obligan a los empleadores a identificar y evaluar continuamente los riesgos laborales, implementar medidas de prevención, y supervisar la correcta utilización de EPPs, además de la correcta y segura ejecución de las labores. La analítica de video con sistemas de IA contribuye al cumplimiento de estas normas, así como la mejora de los estándares de seguridad y permite una respuesta rápida ante desviaciones, apoyando el mejoramiento continuo del sistema de gestión de SST.

Sin embargo, la implementación de estas tecnologías puede generar riesgos psicosociales debido a la percepción de vigilancia constante. Para mitigar estos efectos, es crucial incluir este aspecto en los monitoreos psicosociales que el empleador está obligado legalmente a realizar conforme a la Ley de SST, analizar los signos de estrés o ansiedad y comparar los datos con los obtenidos antes de la implementación de la tecnología, además de implementar las recomendaciones que se determinen sobre la base de los resultados. Es fundamental mantener una

comunicación abierta y transparente con los trabajadores sobre el propósito de la videovigilancia, capacitarlos y sensibilizarlos sobre sus beneficios para su salud y seguridad, así como la de los terceros.

Como vemos en el caso del ejemplo expuesto el uso de IA en materia de SST optimiza el cumplimiento de estas obligaciones del empleador. Pero para su aplicación debe cumplir rigurosamente con el principio de proporcionalidad, los de finalidad y deber de información en el marco de las disposiciones de los datos personales, así como garantizar el respeto irrestricto al derecho fundamental a la privacidad de los trabajadores. La implementación de IA debe ser limitada a las áreas y actividades de mayor riesgo, asegurando que el monitoreo no se extienda innecesariamente a otros aspectos de la vida laboral. Además, los datos recolectados deben ser manejados bajo estrictos protocolos de protección, garantizando que su uso sea exclusivamente para fines de SST y no para otros fines que podrían considerarse intrusivos o excesivos, como imponer sanciones disciplinarias sin haber informado previamente al trabajador esta finalidad o para la evaluación de su desempeño, lo cual excedería la finalidad del tratamiento de los datos en el supuesto analizado.

Implementar normativa interna que recoja los principios de transparencia, explicabilidad, minimización de datos personales, supervisión humana en decisiones automatizadas importantes garantizará que los trabajadores comprendan el uso, funcionamiento y finalidad de los sistemas de IA generando confianza y promoviendo así una aplicación ética y fiable, al mismo tiempo que se reduciría el riesgo psicosocial asociado a la percepción de una vigilancia constante.

Cuestión distinta será el supuesto donde el empleador realiza un control algorítmico total y de gran intensidad del trabajo mediante la recopilación de grandes cantidades de información del trabajador a través de sistemas de videovigilancia, micrófonos, geolocalización, biometría de reconocimiento facial, teléfonos, seguimiento de correos electrónicos, y navegación en internet en tiempo real que permitiría conocer al trabajador en su fuero interno. Esto podría generar un “clima psicosociológico de control e invasión de su privacidad,” donde los trabajadores son plenamente transparentes ante la empresa, afectando su bienestar psicológico y emocional (Mercader, 2022, p.101).

Un análisis de la necesidad particular para tal intensidad de control seguramente no superaría el principio de proporcionalidad ni el de finalidad del

tratamiento de datos, transgrediendo los derechos fundamentales del trabajador, como el de privacidad.

Ilustra lo anterior un reciente caso donde se aplicó estos principios. La Agencia de Protección de Datos Personales de Hungría, sancionó a una entidad financiera por utilizar sistema de IA para realizar psicoanálisis de las voces de los trabajadores durante la atención telefónica a clientes y detectar el estado emocional de ellos sin la debida transparencia. No se informó adecuadamente sobre la finalidad de este tratamiento a los trabajadores ni se realizó una evaluación de la necesidad y proporcionalidad de esta práctica. (Muñoz Ruiz, 2024, p. 151-152).

Como vemos la aplicación de sistemas de IA materializa innegables beneficios si es correctamente aplicado, así como el control permanente plantea desafíos legales como los señalados que deben ser analizados caso por caso, ponderando los derechos fundamentales de los trabajadores, frente a los intereses legítimos del empleador en el uso de estos sistemas. Por ello, cualquier medida adoptada por el empleador debe ser adecuada, necesaria y proporcional en sentido estricto para lograr su objetivo sin afectar los derechos de los trabajadores.

III. CONCLUSIÓN

La IA está revolucionando el entorno laboral, automatizando tanto tareas rutinarias como complejas. Este cambio, aunque promueve la eficiencia y productividad, también requiere una reconfiguración de las habilidades laborales. El empleador debe invertir en formación continua y el desarrollo de competencias tecnológicas para asegurar la competitividad y mitigar el riesgo de desplazamiento laboral. La incorporación de IA en la gestión de trabajadores presenta importantes desafíos éticos y legales, como la invasión de la privacidad y la perpetuación de sesgos discriminatorios. Es esencial establecer un marco legal robusto que regule el uso de la IA en el trabajo, garantizando la transparencia, la explicabilidad, minimización de datos personal y una supervisión humana constante en los procesos críticos.

La IA ofrece herramientas avanzadas para mejorar la SST mediante el monitoreo en tiempo real y la detección precoz de riesgos. Sin embargo, esta tecnología también puede intensificar la vigilancia y generar riesgos psicosociales, afectando la salud mental de los trabajadores. Los empleadores deben equilibrar el uso de la IA con políticas que respeten la privacidad y realicen evaluaciones constantes de estos riesgos. Dada la rápida evolución de la IA, las normativas

laborales deberían actualizarse de forma dinámica para abordar los nuevos desafíos tecnológicos. Las regulaciones deben garantizar la transparencia y explicabilidad, la supervisión humana en las decisiones automatizadas significativa y la mitigación de riesgos, asegurando un uso ético y responsable de la IA que proteja los derechos fundamentales de los trabajadores.

Los empleadores deberían adoptar políticas internas que regulen el uso de la IA de manera ética y conforme a los estándares más altos de protección de derechos laborales. Estas políticas deben centrarse en la seguridad, transparencia, mitigación de riesgos, privacidad, ausencia de sesgos, explicabilidad, minimización de uso de datos personales y supervisión humana. Al hacerlo, no solo se fortalecerá la confianza en el uso de la IA con los beneficios que implica, sino que también se asegurará un entorno laboral justo, seguro y respetuoso de los derechos humanos y laborales.

IV. BIBLIOGRAFÍA

- Acuña Bozo, E. (2024). Inteligencia artificial aplicada a la seguridad y salud en el trabajo. Conferencia magistral presentada en la Semana de la Ingeniería en Perú, Colegio de Ingenieros del Perú - Consejo Departamental de Lima - Capítulo de Ingeniería Sanitaria e Higiene y Seguridad Industrial - CISAHEHSI, Lima, Perú. Recuperado de https://youtu.be/crr_N9gOCLc?si=h-k47I_cqZ0KzPd1
- Aloisi, Antonio and Gramano, Elena, Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context (June 10, 2019). Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection", edited by Valerio De Stefano, Vol. 41, No. 1, pp. 95-121, Available at SSRN: <https://ssrn.com/abstract=3399548>
- Casar Corredera, J. R. (2023). Inteligencia artificial generativa. *Anales de la Real Academia de Doctores de España*, 8(3), 475-489.
- Cazzaniga, F., & otros. (2024). "Gen-AI: Artificial Intelligence and the Future of Work." IMF Staff Discussion Note SDN2024/001, Fondo Monetario Internacional, Washington, DC.
- Corvalán, J. G., Sánchez Caparrós, M., Raban, M., Stringhini, A., Papini, C. M., Heleg, G., & Bonato, V. (2023). Propuestas de regulación y recomendaciones de inteligencia artificial en el mundo. Pontificia Universidad Católica de Argentina. Recuperado de https://www.researchgate.net/publication/372215967_Propues

- tas_de_regulacion_y_recomendaciones_de_inteligencia_artificial_en_el_mundo.
- Dastin, J. (2018, October 10). Insight - Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/>
- Delfanti, A. 2019. “Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse”, in *New Media & Society*, vol. 23 (1): 39–55.
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Recuperado de https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-inteligencia/?utm_source=enlace
- IBM. (2023). Why AI governance is a business imperative for scaling enterprise artificial intelligence. International Data Corporation. Recuperado de https://proassetspdldcom.cdnstatics2.com/usuaris/libros_contenido/arxiu/40/39307_Inteligencia_artificial.pdf
- IBM. (2024). ¿Qué es la inteligencia artificial (IA)? Recuperado de <https://www.ibm.com/mx-es/topics/artificial-intelligence>
- Macías García, M. del C. (2023). La inteligencia artificial. Custodia de la seguridad y salud de las personas trabajadoras. e-Revista Internacional de la Protección Social, (Núm. extraordinario), <https://dx.doi.org/10.12795/e-RIPS>. Universidad de Sevilla.
- Mateescu, A., & Nguyen, A. (2019). Algorithmic management in the workplace. *Data & Society*. Recuperado de https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf
- Mercader Uguina, J. R. (2022). Algoritmos e inteligencia artificial en el derecho digital del trabajo. Tirant lo Blanch.
- Menor, P. (2024, 19 de julio). Implicaciones del Reglamento de IA de la UE en el ámbito laboral. El Confidencial. Recuperado de https://blogs.elconfidencial.com/juridico/tribuna/2024-07-19/implicaciones-reglamento-ia-ue-laboral_3925823/
- Muñoz Ruiz, A. B. (2023). Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales. Tirant lo Blanch. (pp. 151-152)
- OCDE (2023), *Employment Outlook 2023: Artificial Intelligence and the Labour Market*, OECD Publishing, Paris, <https://doi.org/10.1787/08785bba-en>.
- OCDE (2024), “Uso de IA en el lugar de trabajo: oportunidades, riesgos y respuestas políticas”, *OECD Artificial Intelligence Papers*, No. 11, OECD Publishing, París, <https://doi.org/10.1787/73d417f9-en>.

- OCDE (2024), “Memorándum explicativo sobre la definición actualizada de la OCDE de un sistema de IA”, Documentos de Inteligencia Artificial de la OCDE , n.º 8, OECD Publishing, París, <https://doi.org/10.1787/623da898-en> .
- Palomeque, Manuel (2011) “Derecho del trabajo e ideología” Editorial Tecnos 7 Edición 2011.
- Rouhiainen, L. (2018). Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro (pp. 22). Editorial Planeta.
- Rouhiainen, L. (2018). Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro (pp. 17-19). Editorial Planeta.
- Todolí-Signes, Adrian, (2019). En cumplimiento de la primera Ley de la robótica: Análisis de los riesgos laborales asociados a un algoritmo/inteligencia artificial dirigiendo el trabajo (Complying With the First Law of Robotics: An Analysis of the Occupational Risks Associated With Work Directed by an Algorithm/ Artificial Intelligence) (December 19, 2019). Labour & Law Issues, 5 (2), disponible en SSRN: <https://ssrn.com/abstract=3506584>
- Todolí-Signes, Adrian (2022) «La inteligencia artificial no te robará tu trabajo, sino tu salario. Retos del Derecho del Trabajo frente a la dirección algorítmica del trabajo», El Cronista, núm. 100, (pp. 155 y 156)
- Wood, AJ, Gestión algorítmica: consecuencias para la organización del trabajo y las condiciones laborales, Sevilla: Comisión Europea, 2021, JRC124874.
- Sanguinetti, W. (2024). *Los dilemas de los derechos colectivos en la era de la inteligencia artificial*. Trabajo y Derecho, (pp. 115-116). Recuperado de <https://wilfredosanguinetti.wordpress.com/wp-content/uploads/2024/07/w-sanguinetti-los-dilemas-de-los-derechos-colectivos-en-la-era-de-la-inteligencia-artificial-trabajo-y-derecho-2024-numero-115-116.pdf>
- Sanguinetti, W. (2008). La Reconstrucción Jurisprudencial del Derecho del Trabajo en la experiencia del Tribunal Constitucional Peruano. Derecho & Sociedad, (30), 75-83. Recuperado a partir de <http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/17330>
- Silver, David., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., ... & Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. *Nature*, 529(7587), 484-489. <https://doi.org/10.1038/nature16961>
- Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson Higher Ed. ISBN 1292401176, 9781292401171.
- UNESCO (2021) Recomendación sobre la ética de la inteligencia artificial. Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Unión Europea. (2024). Ley de IA de la UE: primera normativa sobre inteligencia artificial. Recuperado de <https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial>