

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL: DESAFÍOS JURÍDICOS PARA LA TUTELA DE LOS DERECHOS FUNDAMENTALES EN EL PERÚ

ARTIFICIAL INTELLIGENCE AND DATA PROTECTION IN THE WORKPLACE: LEGAL CHALLENGES FOR THE PROTECTION OF FUNDAMENTAL RIGHTS IN PERU

ÁNGEL LUIS DELGADO DE LA MATTÁ *

RESUMEN

La digitalización de las relaciones laborales ha intensificado el tratamiento masivo de datos personales mediante inteligencia artificial. Este artículo analiza sus implicancias jurídicas en el ordenamiento peruano en el marco constitucional, legal y jurisprudencial, así como estándares internacionales. Se examina la tensión entre el poder de dirección del empleador y la autodeterminación informativa del trabajador, a la luz de los principios de proporcionalidad, finalidad y transparencia. Asimismo, se identifican riesgos relevantes, como vigilancia excesiva, sesgo algorítmico, opacidad decisional y pérdida de control del titular. Metodológicamente, se emplea un enfoque dogmático, analítico y comparado. Los resultados proponen criterios interpretativos orientados a armonizar innovación tecnológica y tutela efectiva de derechos fundamentales, bajo el enfoque de trabajo decente y gobernanza responsable en la era digital. Se concluye que la inteligencia artificial exige regulación dinámica, capacitación institucional y compromiso empresarial con la dignidad y la protección de datos en el ámbito laboral peruano contemporáneo.

* Jurista con Maestría en Derecho del Trabajo y Seguridad Social de la Universidad Nacional Mayor de San Marcos (Perú). Presidente Filial Perú de la Asociación Iberoamericana de Derecho del Trabajo y de la Seguridad Social – Guillermo Cabanellas. Árbitro Laboral Público y Privado registrado en el Ministerio de Trabajo y Promoción del Empleo del Perú. ORCI: <https://orcid.org/0009-0005-1549-7114> Correo: aidtssfilialperu@gmail.com

PALABRAS CLAVE: Protección de datos personales; inteligencia artificial; autodeterminación informativa; derechos fundamentales; Derecho del Trabajo.

ABSTRACT

The digitalization of labor relations has intensified the large-scale processing of personal data through artificial intelligence. This article examines its legal implications within the Peruvian legal system from constitutional, statutory, and jurisprudential perspectives, as well as under international standards. It analyzes the tension between the employer's managerial power and the worker's informational self-determination in light of the principles of proportionality, purpose limitation, and transparency. Furthermore, it identifies significant risks, including excessive surveillance, algorithmic bias, decision-making opacity, and loss of data subject control. Methodologically, the study adopts a dogmatic, analytical, and comparative approach. The results propose interpretative criteria aimed at harmonizing technological innovation with the effective protection of fundamental rights, under the framework of decent work and responsible governance in the digital era. It concludes that artificial intelligence requires dynamic regulation, institutional training, and corporate commitment to dignity and personal data protection within the contemporary Peruvian labor context.

KEYWORDS: Personal data protection; artificial intelligence; informational self-determination; fundamental rights; Labor Law.

ABREVIATURAS

CP	Constitución Política del Perú
LPDP	Ley de Protección de Datos Personales del Perú
ANPDP	Autoridad Nacional de Protección de Datos Personales

RGPD	Reglamento General de Protección de Datos
TC	Tribunal Constitucional
IA	Inteligencia Artificial
STC	Sentencia del Tribunal Constitucional
HD	Habeas Data
PA	Proceso de Acción de Amparo

1. INTRODUCCIÓN

La digitalización de las relaciones laborales ha transformado estructuralmente la organización, supervisión y evaluación del trabajo, situando al tratamiento de datos personales como un elemento central del vínculo laboral contemporáneo. Desde la selección hasta la extinción del contrato, los empleadores gestionan información personal mediante sistemas crecientemente automatizados, lo que plantea desafíos jurídicos complejos para la tutela de los derechos fundamentales del trabajador.

En este contexto, la protección de datos personales se configura como un derecho fundamental autónomo, vinculado a la dignidad humana y al principio de autodeterminación informativa, que garantiza al titular el control sobre el uso y circulación de su información. Su función trasciende la esfera privada, al constituir un presupuesto para la efectividad de derechos como la intimidad, la igualdad y la no discriminación.

El desarrollo tecnológico ha optimizado la gestión empresarial, pero también ha incrementado riesgos relevantes, tales como la vigilancia excesiva, la toma de decisiones automatizadas, la discriminación algorítmica y la pérdida de control informativo. La inteligencia artificial aplicada a procesos laborales acentúa estas tensiones, debido a la opacidad de los algoritmos y la reproducción de sesgos estructurales.

En el Perú, la Ley No. 29733 establece el marco general de protección de datos, plenamente exigible en el ámbito laboral, aunque su desarrollo normativo y jurisprudencial no siempre avanza al ritmo de la innovación tecnológica. El Tribunal

Constitucional ha reconocido la autodeterminación informativa como derecho fundamental relacional, exigible frente a usos arbitrarios o desproporcionados.

El presente artículo analiza las implicancias jurídicas de la inteligencia artificial en el tratamiento de datos laborales, identifica riesgos y vacíos normativos, y propone criterios interpretativos orientados a armonizar la innovación tecnológica con la tutela efectiva de los derechos fundamentales, bajo un enfoque de trabajo decente y gobernanza responsable en la era digital.

2. SISTEMA NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ: UN DERECHO LABORAL FUNDAMENTAL

2.1. MARCO NORMATIVO NACIONAL

El derecho fundamental a la protección de datos personales encuentra en el ordenamiento jurídico peruano su primer reconocimiento en la Constitución Política de 1993, como manifestación concreta de la tutela de la dignidad humana, valor supremo del Estado Constitucional de Derecho. En ese sentido, la Constitución Política de 1993 del Perú, en su Artículo 2°, inciso 6) establece que: “Toda persona tiene derecho: “A que los servicios informáticos computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar”,¹ consagrando así una garantía constitucional frente al tratamiento indebido de información personal. Este reconocimiento situó al Perú, en el contexto latinoamericano, entre los Estados pioneros en constitucionalizar la protección de datos personales, anticipando su posterior consolidación legislativa y jurisprudencial como derecho fundamental autónomo.

En esa línea, Aguilera Izquierdo (2020) señala que “La protección de datos se concibe en nuestra Constitución como un instrumento de garantía de otros derechos fundamentales, la

¹ Constitución Política del Perú (2025). Ministerio de Justicia y Derechos Humanos, Vigésima edición oficial. pp. 27-30. <https://cdn.www.gob.pe/uploads/document/file/8775223/7255126-vigesima-constitucion-2025-08-25.pdf?v=1759507534>

intimidad y el honor, pero también como un instituto que es en sí mismo un derecho o libertad fundamental. Nos encontramos, por tanto, ante un derecho fundamental específico que coexiste con la función de garantía instrumental de otros derechos”.²

Posteriormente, el 2011 en cumplimiento del mandato constitucional, se promulgó la Ley No. 29733, Ley de Protección de Datos Personales, aplicable a los sectores público y privado. Aunque no es una norma laboral en sentido estricto, su observancia es obligatoria en las relaciones de trabajo, dado que el empleador actúa como responsable del tratamiento de los datos personales de sus trabajadores. El marco reglamentario de la LPDP fue inicialmente desarrollado por el Decreto Supremo No. 003-2013-JUS, vigente hasta el 30 de marzo de 2025. A partir de dicha fecha, entró en vigor el Decreto Supremo No. 016-2024-JUS,³ que actualiza el régimen de protección de datos personales con el objetivo de responder a los desafíos derivados de la transformación digital, la automatización de procesos y el uso de inteligencia artificial, así como de armonizar la normativa nacional con los estándares internacionales de protección.

La LPDP establece principios rectores del tratamiento de datos personales -licitud, finalidad, proporcionalidad, calidad, transparencia y seguridad- cuya observancia adquiere especial relevancia en el ámbito laboral, dada la asimetría estructural de la relación de subordinación y la necesidad de una tutela reforzada del trabajador como titular de los datos. Como regla general, el tratamiento de datos exige el consentimiento previo, informado, expreso e inequívoco del titular. Sin embargo, en el ámbito laboral la LPDP admite una excepción, permitiendo el tratamiento sin consentimiento cuando este resulte necesario y

² Aguilera Izquierdo, R., “El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización.” *Revista de Trabajo y Seguridad Social*. CEF, (442), 2020, 96. <https://doi.org/10.51302/rtss.2020.886>

³ D.S. 016-2024-JUS, Reglamento de la ley de datos personales. <https://cdn.www.gob.pe/uploads/document/file/7756037/6554453-reglamento-de-la-ley-n-29733.pdf?v=1743779969>

proporcional para la ejecución del contrato de trabajo o para el cumplimiento de obligaciones legales del empleador, vinculadas a la gestión de planillas, seguridad social, salud ocupacional y control de asistencia.

Esta excepción no libera al empleador del deber de información, quien debe comunicar de manera clara y accesible la finalidad y condiciones del tratamiento de los datos, bajo responsabilidad por vulneración del principio de transparencia. En cambio, cuando el tratamiento no se relacione directamente con la relación laboral, se exige el consentimiento expreso, libre y específico del trabajador.

El régimen de protección de datos laborales se ve complementado por diversas normas sectoriales y transversales. Entre ellas, destaca el Decreto Legislativo No. 1353,⁴ que fortalece el rol de la Autoridad Nacional de Protección de Datos Personales (ANPDP); el Decreto de Urgencia No. 007-2020,⁵ que aprueba el Marco de Confianza Digital y reconoce la protección de datos como eje central de la seguridad jurídica en entornos digitales; y el Decreto Legislativo No. 1412,⁶ Ley de Gobierno Digital, que incorpora los principios de privacidad desde el diseño y por defecto en los servicios digitales del Estado.

Asimismo, la ANPDP ha emitido la Directiva No. 01-2020-

⁴ Decreto Legislativo No. 1353, crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de Intereses. (2017). Plataforma del Estado Peruano. Pp. 1-7 <https://cdn.www.gob.pe/uploads/document/file/2790446/Decreto%20Legislativo%20N%C2%BA%201353.pdf?v=1643321801>

⁵ Decreto de Urgencia No. 007-2020, que aprueba el Marco de Confianza Digital (2020). Plataforma del Estado Peruano. Pp. 1-4 <https://cdn.www.gob.pe/uploads/document/file/2790485/Decreto%20de%20Urgencia%20N%C2%BA%20007-2020.pdf?v=1643322610>

⁶ Decreto Legislativo No. 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018). Plataforma del Estado Peruano. Pp. 1-5 <https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf?v=1566312763>

JUS/DGTAIPD,⁷ que regula el tratamiento de datos personales mediante sistemas de videovigilancia, estableciendo criterios estrictos de proporcionalidad, finalidad y transparencia, especialmente relevantes en el ámbito laboral. Un hito reciente lo constituye la Ley No. 31814,⁸ Ley Marco de Desarrollo de la Inteligencia Artificial, cuyo reglamento clasifica como de alto riesgo las aplicaciones de IA utilizadas en procesos de selección, evaluación, contratación y cese de trabajadores. Esta calificación refuerza la necesidad de un tratamiento normativo diferenciado y de salvaguardas específicas en materia de protección de datos y no discriminación.

Desde la perspectiva jurisprudencial, el Tribunal Constitucional peruano ha reconocido de manera reiterada que la autodeterminación informativa constituye un derecho fundamental autónomo. En la STC Exp. No. 1797-2002-HD/TC,⁹ el Tribunal afirmó que dicho derecho faculta al individuo a controlar la información que lo identifica, mientras que en la STC No. 00141-2011-PA/TC¹⁰ precisó que todo tratamiento de datos debe sujetarse a los principios de consentimiento, proporcionalidad y finalidad. Adicionalmente, el Código Penal peruano refuerza la tutela de los datos personales mediante la tipificación del delito de tráfico ilegal de datos personales (artículo 154-A),¹¹ sancionando penalmente la comercialización o venta ilegítima de información no pública, incluida aquella de naturaleza laboral.

⁷ Directiva No. 01-2020-JUS/DGTAIPD (2020). Plataforma del Estado Peruano. Pp. 1-24 <https://cdn.www.gob.pe/uploads/document/file/1910249/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf?v=1621961664>

⁸ Ley No. 31814, Ley Marco de Desarrollo de la Inteligencia Artificial (2023). Plataforma del Estado Peruano. Pp. 1-3 <https://cdn.www.gob.pe/uploads/document/file/5038703/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814.pdf?v=1692895308>

⁹ STC Exp. No. 1797-2002-HD/TC <https://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html>

¹⁰ STC No. 00141-2011-PA/TC <https://www.tc.gob.pe/jurisprudencia/2011/00141-2011-AA%20Resolucion.html>

¹¹ Código Penal Peruano (2016). Ministerio de Justicia y Derechos Humanos. Décimo Segunda Edición Oficial. p. 111. <https://cdn.www.gob.pe/uploads/document/file/3621138/C%C3%93DIGO%20PENAL.pdf?v=1663014332>

2.2. MARCO NORMATIVO Y JURISPRUDENCIAL COMPARADO

En el ámbito internacional, el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos – RGPD) constituye el estándar más avanzado y referente obligado en materia de protección de datos personales, incluido el tratamiento en el entorno laboral. Este instrumento reconoce expresamente la naturaleza fundamental del derecho a la protección de datos y establece garantías reforzadas frente a decisiones automatizadas y perfiles basados en tratamiento masivo de información.

Sobre el particular, López Ahumada (2025) en referencia a la intimidad en el ámbito del trabajo digitalizado, en el marco del Reglamento español, señala:

Con carácter general, se suele referir, como medida de respeto del derecho a la intimidad de los trabajadores, a la obligación de la empresa de configurar los dispositivos electrónicos, evitando los registros innecesarios o de carácter permanente de la actividad de los trabajadores. Nos encontramos, pues, con una máxima general en materia de protección de datos, que se refiere a la prevención del propio tratamiento de los datos personales (art. 25.1 y 2 del RGPD).¹²

La jurisprudencia del Tribunal de Justicia de la Unión Europea ha desempeñado un papel central en la delimitación de los límites al poder empresarial. En el caso *Google Spain vs. AEPD y Mario Costeja González* (C-131/12, 2014), el TJUE reafirmó la protección de datos como una manifestación de la dignidad y autonomía personal. Asimismo, en el caso *Barbulescu vs. Rumanía* (2017), se establecieron criterios estrictos sobre el control empresarial de las comunicaciones laborales, enfatizando la necesidad de información previa, proporcionalidad y respeto a la vida privada del trabajador.

¹² López Ahumada, J. E., “El desarrollo de los estándares de protección de la intimidad en el ámbito laboral desde la perspectiva de la tutela de los derechos fundamentales”. *Derechos fundamentales y derecho del trabajo ante el proceso de transformación digital*. Universidad de Alcalá. Departamento de Ciencias Jurídicas. Lucerna Juris. Primera Edición 2024. Pp. 131 y 132. <https://dialnet.unirioja.es/servlet/libro?codigo=1006429>

En la misma línea, el Tribunal Constitucional español, en la STC 292/2000, definió la autodeterminación informativa como un derecho fundamental autónomo que confiere a la persona un poder de disposición y control sobre sus datos, facultándola para decidir cuáles proporcionar, a quién y con qué finalidad.

2.3. CONSIDERACIONES FINALES DEL MARCO NORMATIVO

En suma, el marco normativo peruano se inserta en una tendencia global de fortalecimiento de la tutela de los datos personales, con especial atención al ámbito laboral como espacio particularmente sensible a la vulneración de derechos fundamentales. La convergencia entre normativa nacional, estándares internacionales y desarrollo jurisprudencial evidencia la necesidad de un enfoque integral que permita afrontar los desafíos derivados del uso de tecnologías digitales e inteligencia artificial en las relaciones de trabajo.

3. INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL EN UN CONTEXTO LABORAL DIGITALIZADO

La digitalización de las relaciones laborales ha impulsado el uso de herramientas de inteligencia artificial en los procesos de gestión del talento humano. No obstante, aunque estas tecnologías prometen eficiencia y objetividad, su implementación plantea importantes desafíos para la protección de los derechos fundamentales de los trabajadores, especialmente en materia de datos personales, igualdad de oportunidades e intimidad.

De esta manera López Ahumada (2025) destaca que

[...] el recurso a la inteligencia artificial y a los algoritmos más sofisticados permiten a las empresas nuevas posibilidades en la gestión de sus recursos humanos. Asimismo, estos recursos permiten disponer a las empresas de un conjunto de datos de alto valor vinculados al proceso de producción, que pueden ser objeto de intercambio y que es preciso administrar de la forma más adecuada posible. Toda esta información obliga a las empresas a observar un

estricto proceso de tratamiento y contemplar medidas de uso adecuado desde la perspectiva de la privacidad de los trabajadores.¹³

Los sistemas algorítmicos aplicados a la toma de decisiones laborales pueden reproducir y amplificar sesgos estructurales presentes en los datos de entrenamiento, generando prácticas discriminatorias por razones de edad, género u origen socioeconómico, lo que compromete el principio de igualdad y no discriminación. Asimismo, el uso intensivo de tecnologías de control y monitoreo configura un entorno de vigilancia permanente que incide negativamente en la intimidad, la privacidad y la autodeterminación informativa del trabajador, fortaleciendo de manera desproporcionada el poder de dirección empresarial mediante herramientas de injerencia sin precedentes en la esfera personal. En ese sentido, López Ahumada (2025) refiere que

El aumento del número de dispositivos conectados a las personas trabajadoras permite monitorizar su trabajo mediante distintas aplicaciones y recursos, que proveen a la empresa información relativa a la salud, a sus hábitos y prácticas personales o, en su caso, a su geolocalización, cuando se trata de trabajadores con movilidad laboral. Junto a los datos de carácter personal, también se encuentran otro tipo de informaciones relativas a la dimensión laboral propiamente dicha, mediante la recopilación de datos que informan a la empresa sobre el rendimiento, la actividad y la ejecución del trabajo.¹⁴

En materia de protección de datos personales, el consentimiento constituye la base general de legitimación del tratamiento; sin embargo, en el ámbito laboral dicho consentimiento presenta serias limitaciones de autenticidad, debido a la relación de

¹³ López Ahumada, J.E., “Transformación digital y su repercusión en los derechos fundamentales de las personas trabajadoras”. Preámbulo. Derechos fundamentales y derecho del trabajo ante el proceso de transformación digital. Universidad de Alcalá. Departamento de Ciencias Jurídicas. Lucerna Juris. Primera Edición 2024. Pp. 7-13. <https://dialnet.unirioja.es/servlet/libro?codigo=1006429>.

¹⁴ López Ahumada, op. cit. P. 8. <https://dialnet.unirioja.es/servlet/libro?codigo=1006429>

subordinación que impide al trabajador oponerse libremente sin riesgo de consecuencias desfavorables. En este contexto, resulta cuestionable que pueda calificarse como verdaderamente voluntario un consentimiento cuya negativa puede implicar la exclusión de un proceso de selección o la pérdida de oportunidades profesionales.

En ese sentido, reseñando el deber del empleador de comunicar previamente el uso de los equipos digitalizados a los trabajadores, López Ahumada (2025) sostiene “Con carácter general, podemos decir que el deber de información sobre el empleo de los medios digitales en el trabajo encuentra distintos aspectos problemáticos y que generan inseguridad jurídica”.¹⁵

Por ello, la propia normativa reconoce que el tratamiento de datos personales en el ámbito laboral puede prescindir del consentimiento cuando resulte necesario y proporcional para la ejecución del contrato de trabajo. Sin embargo, esta excepción no puede interpretarse de manera extensiva o arbitraria, pues el consentimiento sigue siendo exigible cuando los datos se utilicen para finalidades extra laborales, tales como actividades publicitarias, comerciales o de marketing, que no guardan relación directa con la relación de trabajo.

En el caso de los datos sensibles, la regla general es aún más estricta: se requiere un consentimiento previo, expreso, informado e inequívoco del titular. La LPDP prohíbe el consentimiento tácito y exige una manifestación clara de voluntad, preferentemente por escrito, admitiéndose en entornos digitales únicamente acciones afirmativas que garanticen información previa suficiente y comprensión efectiva del tratamiento.

Esta exigencia se justifica en la necesidad de evitar tratamientos abusivos amparados en autorizaciones ambiguas o genéricas, como lo sostiene Olivos Celis (2020) que nos precisa

(...) la norma no admite el consentimiento tácito. Más aún,

¹⁵ Lopez Ahumada. Vid. Supra, P. 137. <https://dialnet.unirioja.es/servlet/libro?codigo=1006429>

cuando el tratamiento de datos incluye datos sensibles, el consentimiento debe realizarse según lo exige la propia norma por escrito. En complemento, el artículo 12° del reglamento desarrolla las características del consentimiento obtenido en entornos digitales, señalando en el numeral 3 que en estos casos también se considera expresa la manifestación consistente en “hacer clic”, “clickear” o “pinchar”, “dar un toque”, “touch” o “pad” y otros similares.¹⁶

En cuanto al derecho a la intimidad se desprende, de manera autónoma, el derecho a la confidencialidad y a la protección de los datos personales, cuya tutela adquiere especial complejidad en contextos caracterizados por el *big data*, la interoperabilidad de sistemas y la transferencia transfronteriza de información. La masificación del almacenamiento electrónico y la circulación global de datos incrementan de forma significativa los riesgos de accesos no autorizados, filtraciones, usos incompatibles y elaboración de perfiles automatizados.

En relación a ello, Blancas Bustamante (2021) advierte que los derechos relativos a la dignidad e intimidad del trabajador se encuentran particularmente expuestos a vulneraciones cuando el poder de control empresarial se ejerce de manera desmedida, especialmente debido al uso intensivo de las nuevas tecnologías, las cuales permiten realizar intrusiones cada vez más profundas en la esfera privada del trabajador, por lo que en esa línea, sostiene;

En particular, son los derechos relativos a la dignidad e intimidad del trabajador los que se toman especialmente vulnerables cuando el poder de control se ejerce en forma ilimitada, en la medida que las nuevas tecnologías que se han puesto a su alcance, son capaces de efectuar intrusiones indebidas en la esfera privada de aquel. De allí que resulta indispensable afirmar la eficacia ante el empleador

¹⁶ Olivos Celis, M., “El camino del derecho a la protección de datos personales en el Perú tras su incorporación en la constitución política de 1993”. IUS Revista de Investigación de la Facultad de Derecho. 2020. Universidad Católica Santo Toribio de Mogrovejo - Chiclayo, Perú. US Vol. 9. No. 1. Pp. 83-100. <http://doi.org/10.35383/ius-usat.v9i1.338>

(eficacia horizontal o inter-privatos) de aquellos derechos fundamentales que tienen por objeto tutelar la esfera privada, la vida personal del trabajador, como es el caso de los que están reconocidos en los numerales 6, 7, 10 Y 18 del artículo 2º de la Constitución.¹⁷

En este escenario, la revolución digital 5.0 y el uso intensivo de las NTIC no pueden legitimar la precarización ni la regresión de los derechos fundamentales de los trabajadores. Por el contrario, corresponde al ordenamiento jurídico establecer un marco normativo que garantice el trabajo decente, la progresividad de los derechos y la interdicción de la arbitrariedad en el uso de la inteligencia artificial y de las tecnologías digitales. Ello exige, además, mecanismos de equilibrio que, sin desconocer los legítimos intereses empresariales, aseguren que las medidas de vigilancia y control sean excepcionales, necesarias y proporcionales, en armonía con los principios de dignidad humana y justicia social. En definitiva, la protección de los datos personales en contextos de inteligencia artificial no constituye un límite a la innovación, sino una condición esencial para el desarrollo de un modelo de relaciones laborales compatible con el Estado constitucional de derecho y con una tecnología centrada en la persona.

4. RIESGOS Y PROBLEMÁTICAS EN LA PROTECCIÓN DE DATOS EN EL ENTORNO LABORAL DIGITALIZADO

La incorporación de las tecnologías de la información, la inteligencia artificial y los sistemas algorítmicos ha generado un escenario ambivalente en el ámbito laboral: si bien incrementan la eficiencia y competitividad empresarial, también intensifican las capacidades de vigilancia y control del empleador, tensionando derechos fundamentales del trabajador como la intimidad, la igualdad y la autodeterminación informativa.

¹⁷ Blancas, C., “Poder de dirección y derecho a la intimidad y privacidad del trabajador.” *Revista de la sociedad peruana de derecho del trabajo y de la seguridad social*. 2021, p. 160. <https://www.sptdss.org.pe/wp-content/uploads/2021/09/Laborem10-147-174.pdf>

En este contexto, la protección de datos personales no busca eliminar el poder de dirección empresarial, sino someterlo a un ejercicio constitucionalmente legítimo, conforme a los principios de proporcionalidad, razonabilidad, finalidad y minimización. La legitimidad del control depende de que las medidas adoptadas sean idóneas, necesarias y estrictamente proporcionales.

4.1. DIGITALIZACIÓN DEL ESTADO Y ACUMULACIÓN MASIVA DE DATOS

La digitalización estatal amplía los riesgos asociados a la acumulación, interoperabilidad y transferencia de grandes volúmenes de datos personales, incrementando la exposición a brechas de seguridad, usos indebidos, tratamiento de datos biométricos y geolocalización sin controles suficientes, agravados por limitaciones presupuestales y deficiencias de capacitación.

En el Perú, el derecho a la intimidad y a la autodeterminación informativa se reconoce en el artículo 2, inciso 6, de la Constitución, y se desarrolla en la Ley N.º 29733 y su Reglamento actualizado por el Decreto Supremo N.º 016-2024-JUS. No obstante, la eficacia del sistema aún presenta importantes déficits frente a los desafíos tecnológicos.

4.2. RIESGOS EN EL ÁMBITO JUDICIAL LABORAL

En los procesos laborales, la solicitud de exhibición de documentos por parte del trabajador plantea riesgos relevantes para la protección de datos personales. La admisión de dichos medios probatorios corresponde al juez, quien debe evaluar su pertinencia, necesidad y proporcionalidad, garantizando un adecuado equilibrio entre el derecho a la prueba y el derecho fundamental a la protección de datos personales.

Como advierte Lora (2025),

Este tipo de situación a la que nos referimos son los procesos judiciales de naturaleza laboral, en donde es común que la

parte demandante (trabajador o extrabajador) solicite como medio probatorio la exhibición de documentación que obra en poder del empleador. Por ejemplo, el trabajador que demanda puede aportar como medio probatorio que el empleador (demandado) exhiba boletas de pago, contratos u otros documentos pertinentes. Sin embargo, es importante entender que no basta con que el trabajador solicite la exhibición de documentación, sino, es el juez quien debe evaluar y admitir la solicitud de exhibición documental en la etapa probatoria del proceso”.¹⁸

En ese orden, se coincide con esta opinión, al sostener que, en la práctica, muchos empleadores adjuntan unilateralmente tales documentos laborales al contestar la demanda, incluso cuando contienen datos personales propios y de terceros ajenos al proceso, como de otros trabajadores, extrabajadores, proveedores o empresas vinculadas. Esta actuación, pese a estar motivada por una aparente colaboración procesal, puede configurar una vulneración a la normativa de protección de datos personales. Desde una perspectiva jurídica, el empleador no se encuentra obligado a exhibir documentos con datos de terceros sin mandato judicial expreso; sin embargo, esta exigencia suele ser ignorada en la dinámica cotidiana de los procesos tramitados ante los Juzgados y Salas laborales del país.

Por su parte, en palabras de Torres Montano (2025)

El reconocimiento judicial de la autodeterminación informativa y del olvido fortalece el énfasis constitucional en la privacidad y exige medidas proactivas (encriptado, eliminación, etc.) por parte de las entidades públicas. Estos desarrollos subrayan la necesidad de que la administración pública incorpore, en su gobierno digital, mecanismos efectivos de protección desde el diseño coincidiendo con lo que dispone el DL

¹⁸ Lora, G., Protección de datos personales y procesos judiciales de naturaleza laboral. 2025. Consultada el 18 de enero del 2026. <https://aperhu.pe/proteccion-de-datos-personales-y-procesos-judiciales-de-naturaleza-laboral/>

1412 –y promueva el correcto ejercicio de los derechos ARCO de los ciudadanos.¹⁹

Por otro lado, hace un balance entre el derecho a la información pública y balance con datos sensibles y establece que

[...] el derecho constitucional de acceso a la información pública (art. 2.5 CP) impone a las entidades del Estado la obligación de proveer datos a cualquier ciudadano que lo solicite, salvo excepciones legalmente previstas; la ley de transparencia (Ley 27806) y su reglamento confirman este principio de máxima publicidad. Sin embargo, surge un punto de fricción cuando la información requerida incluye datos personales sensibles.²⁰

4.3. BRECHA ENTRE LA NORMA Y LA REALIDAD

Diversos informes de la Autoridad Nacional de Protección de Datos Personales evidencian una significativa brecha entre el marco normativo y su aplicación efectiva.

Según datos citados por Sipión Castillo (2025), menos del 50% de las empresas inspeccionadas cuenta con políticas específicas para el tratamiento de datos personales en el ámbito laboral. En ese sentido, señala que “Según un informe de la ANPDP de 2023, el 78% de los trabajadores ha proporcionado información sensible, como historial médico o situación crediticia, en procesos laborales. Además, el 56% de las empresas utiliza herramientas digitales para supervisar actividades laborales, lo que plantea preocupaciones significativas sobre privacidad.”²¹

Además, sostiene que entre las vulneraciones más recurrentes

¹⁹ Torres Montano, R, “Gobierno digital y protección de datos personales en la administración pública peruana”. Revista Sapere Facultad de Derecho –USMP. Vol. 1 Núm. 28. P. 7. 2025, <https://portalrevistas.aulavirtualusmp.pe/index.php/SP/article/view/3271/4039>

²⁰ Ibidem. P 7. <https://portalrevistas.aulavirtualusmp.pe/index.php/SP/article/view/3271/4039>

²¹ Sipión Castillo, G. “Protección de datos personales ,en el ámbito laboral. *Polemos, portal jurídico* interdisciplinario”. 2025. Consultado el 18 de enero del 2026. <https://polemos.pe/proteccion-de-datos-personales-en-el-ambito-laboral/>

se identifican: el acceso no autorizado a bases de datos, la recopilación de información irrelevante para la relación laboral, la ausencia de consentimiento informado y la falta de transparencia en el tratamiento de la información. Estas prácticas afectan con mayor intensidad a trabajadores tercerizados, personas con discapacidad y postulantes a empleo, cuyas redes sociales son frecuentemente evaluadas sin criterios claros, objetivos ni éticos.

4.4. COMERCIALIZACIÓN DE DATOS Y ECONOMÍA DIGITAL

Desde una perspectiva estructural, se advierte que la regulación resulta ineficaz frente a la comercialización masiva de datos personales por parte de los gigantes tecnológicos. Empresas como Google, Facebook o Apple ofrecen servicios aparentemente gratuitos, cuando en realidad el modelo de negocio se sustenta en la explotación económica de la información personal de los usuarios, quienes rara vez otorgan un consentimiento libre, informado y consciente (Cubillos Vélez. 2017) “La ineficacia de la regulación actual obedece en gran parte a la comercialización de los datos realizada por los gigantes de internet. Empresas como Facebook, Google o Apple proponen un servicio gratuito al internauta; sin embargo, detrás de esta gratuidad se esconde una finalidad económica. De manera que la gratuidad sólo es aparente y la audiencia, es decir, el titular de los datos personales, será conducido sutilmente a no darse cuenta del consentimiento otorgado”.²²

El fenómeno de la publicidad dirigida, basada en el análisis del comportamiento digital del usuario, ilustra con claridad esta problemática. Las búsquedas realizadas por un internauta determinan la orientación posterior de la publicidad, mediante sistemas automatizados de subasta en tiempo real.

²² Cubillos Vélez A., La explotación de los datos personales por los gigantes de internet. *Revista de la Biblioteca Jurídica Virtual* del Instituto de Investigaciones Jurídicas de la UNAM. P. 37, 2017. . <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>

En la práctica, la mayoría de los usuarios nunca ha consentido expresamente este tratamiento, lo que cuestiona seriamente su compatibilidad con los principios de licitud del tratamiento de datos.

A ello se suma el uso generalizado de cookies, que permiten identificar al titular de la información y constituyen, por tanto, un tratamiento de datos personales. Muchas de estas herramientas operan bajo mecanismos de aceptación forzada, sin ofrecer una alternativa real de rechazo, lo que vulnera el principio de consentimiento libre exigido por la legislación peruana. Al respecto, Cubillos Vélez sostiene que

[...] La instalación de cookies constituye un tratamiento de datos personales, toda vez que estas informaciones permiten identificar al titular de la información. La cantidad de cookies que se instalan durante la navegación en internet es considerable. Existen varias cookies que no cumplen con todas las exigencias de un consentimiento libre, expreso e informado. Otras se contentan con informar al titular que se instalarán cookies mediante una ventana emergente, condicionando la navegación a la aceptación de su instalación. Estas ventanas emergentes no permiten rechazar la instalación de cookies y se cierran inmediatamente. Ninguna actividad en internet debería ser subordinada a la autorización del titular para suministrar datos personales.²³

4.5. INTELIGENCIA ARTIFICIAL Y DÉFICIT DE CUMPLIMIENTO NORMATIVO

En este escenario, los tratamientos de datos personales efectuados mediante sistemas de inteligencia artificial no se ajustan plenamente a las condiciones de licitud previstas en la normativa peruana vigente. Así lo explican Urrutia y Valencia (2024) “[...] en nuestro país no contamos con un

²³ Ibidem. P. 38. <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>

ordenamiento jurídico que contemple expresamente la protección de datos personales ante el uso de Tecnologías de la Información y Comunicación (en adelante TIC), específicamente aquellas que se realicen en el marco del poder de fiscalización del empleador como las de monitoreo digital por GPS o videovigilancia”.²⁴ Paradójicamente, pese a la claridad normativa, en el Perú aún no se registran sanciones significativas por este tipo de prácticas, lo que contribuye a una cultura de incumplimiento estructural.

4.6. SÍNTESIS CRÍTICA

En suma, la protección de datos personales en el entorno laboral y digital se encuentra atravesando una tensión permanente entre eficiencia tecnológica, intereses económicos y tutela efectiva de los derechos fundamentales. La intimidad, la dignidad y la autodeterminación informativa del trabajador no pueden quedar subordinadas a la lógica de mercado ni al avance irreflexivo de la tecnología. En base a esta problemática en el entorno laboral digitalizado, Zamudio Salinas (2021), expresa:

En el Perú no ha existido una norma específica sobre protección de datos personales aplicables al ámbito laboral y menos que regule el tratamiento de los datos personales de los trabajadores sometidos al control empresarial; por lo que se hace necesario conocer en qué medida la legislación, y la jurisprudencia han atendido esta situación de desequilibrio entre el derecho de los trabajadores a la protección de sus datos personales y la facultad

²⁴ Urrutia Zamalloa, J. & Valencia Castillo, R., "La protección de datos personales de los trabajadores frente al uso de tecnologías de monitoreo GPS y videovigilancia en el entorno laboral". Trabajo de Suficiencia Profesional presentado en satisfacción parcial de los requerimientos para obtener el título profesional de Abogado. Universidad ESAN. Facultad de Derecho y Ciencias Sociales carrera de Derecho Corporativo. P. 48. 2024. <https://repositorio.esan.edu.pe/server/api/core/bitstreams/421ced9b-0f71-40e0-9549-729f35d4893d/content>

de control del empresario, quien usa para el ejercicio de dicha potestad de las TIC [...]”²⁵

El derecho a la protección de datos no es absoluto, pero sus límites solo pueden encontrarse en otros derechos y bienes constitucionalmente protegidos, y no en intereses meramente económicos o empresariales, como lo señala Conde Ortiz (2005), quien destaca que, “El derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga límites específicos, ni remita a los Poderes Públicos para su determinación, los límites han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos.”²⁶ En consecuencia, el desafío contemporáneo consiste en construir un modelo de gobernanza digital que armonice la innovación tecnológica con la centralidad de la persona humana, como eje del Estado constitucional y del derecho del trabajo.

5. ACTORES INSTITUCIONALES EN LA PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ

La protección efectiva de los datos personales no depende únicamente de la existencia de un marco normativo, sino de la actuación coordinada de las instituciones públicas encargadas de garantizar su cumplimiento. En el Estado constitucional, estas entidades cumplen una función esencial de tutela, fiscalización, promoción y control, orientada a asegurar el ejercicio real y no meramente formal del derecho fundamental a la autodeterminación informativa.

²⁵ Zamudio Salinas, M., “El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. límites y propuestas”. Tesis para optar el grado académico de Magister en Derecho con mención en Derecho Constitucional. P. 79, 2021 <https://tesis.pucp.edu.pe/server/api/core/bitstreams/a574e4d8-a030-4192-97d4-3f7bdf5ee22a/content>

²⁶ Conde Ortiz, C., “La protección de datos personales: Un derecho autónomo con base en los conceptos de intimidad y privacidad”. Universidad de Cádiz. Editorial Dykinson, S.L. Madrid, 2005, P. 47. <https://rodin.uca.es/handle/10498/26396>

5.1. EL ROL DE LAS AUTORIDADES PÚBLICAS

Las autoridades administrativas desempeñan un papel central no solo desde una función sancionadora, sino principalmente desde una función promocional del derecho fundamental a la protección de datos. En este sentido, las campañas de concientización, la información al ciudadano, la elaboración de guías técnicas, la cooperación interinstitucional y la articulación con los sistemas educativos constituyen instrumentos indispensables para acercar progresivamente a la ciudadanía al conocimiento y ejercicio efectivo de este derecho. En palabras de Martínez Martínez (2007)

En primer lugar, las autoridades juegan un papel esencial desde el punto de vista de la función promocional insita en el conjunto de competencias que les atribuye la legislación sectorial. En tal sentido, las campañas de concienciación, la información al ciudadano, la generación de herramientas e instrumentos documentales, –guías, folletos etc.–, y la colaboración con otras administraciones como la municipal y/o la educativa deben acercar cada vez más al ciudadano al conocimiento del derecho fundamental a la protección de datos”.²⁷

Para Torres Montano (2025), “los desafíos y riesgos en la práctica en la administración pública y en el marco del Gobierno Digital destaca que: La proliferación de servicios digitales y el incremento en la recolección de datos plantean múltiples riesgos de vulneración de derechos fundamentales en el ámbito público”.²⁸

Y concluye destacando que

La expansión del gobierno digital en el Perú presenta una oportunidad histórica para mejorar la gestión pública, pero simultáneamente conlleva desafíos significativos en la protec-

²⁷ Martínez Martínez, R., “El derecho fundamental a la protección de datos: perspectivas.” Monográfico III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas. Revista de Internet, Derecho y Política. No. 5. Universitat Oberta de Catalunya. 2007, P. 60. <https://www.redalyc.org/pdf/788/78812861005.pdf>

²⁸ Torres, R., op. cit. P. 9. <https://portalrevistas.aulavirtualusmp.pe/index.php/SP/article/view/3271/4039>

ción de los datos personales; el análisis doctrinario desarrollado evidencia que el país dispone ya de un marco normativo sólido integrado por la Constitución, la Ley 29733 y su reciente reglamento, así como la Ley de Gobierno Digital que articula la protección de datos con los principios constitucionales de privacidad y transparencia. La jurisprudencia del Tribunal Constitucional ha avanzado en la interpretación de estos derechos, subrayando la responsabilidad estatal en garantizar la intimidad de la información y estableciendo criterios claros de equilibrio con la publicidad informativa.²⁹

5.2. AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

En el Perú, la Autoridad Nacional de Protección de Datos Personales (ANPDP) es ejercida por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, en coordinación con la Autoridad Nacional de Transparencia. Entre sus principales competencias se encuentran: resolver en última instancia los procedimientos administrativos sancionadores, conocer y resolver los reclamos por vulneración de los derechos ARCO, administrar el Registro Nacional de Protección de Datos Personales, Supervisar flujos transfronterizos de datos, inscribir, fiscalizar y cancelar bancos de datos públicos y privados, emitir directivas de seguridad de la información e imponer y ejecutar sanciones administrativas.

El artículo 35 de la LPDP impone un deber estricto de confidencialidad a su personal, lo que refuerza la legitimidad institucional y la confianza ciudadana. No obstante, la eficacia de la ANPDP enfrenta limitaciones estructurales relacionadas con recursos presupuestales, especialización técnica y una cultura empresarial aún insuficientemente comprometida con el cumplimiento normativo.

²⁹ Torres, R. op. cit. P. 13. <https://portalrevistas.aulavirtualusmp.pe/index.php/SP/article/view/3271/4039>

5.3. SUNAFIL Y LA TUTELA LABORAL DE LOS DATOS PERSONALES

En el ámbito sociolaboral, la Superintendencia Nacional de Fiscalización Laboral (SUNAFIL) cumple un rol complementario pero decisivo en la protección de los datos personales de los trabajadores. Como órgano rector del sistema inspectivo, supervisa el cumplimiento del ordenamiento jurídico laboral, incluyendo la observancia de la LPDP cuando el tratamiento de datos incide en derechos fundamentales del trabajador.

SUNAFIL puede intervenir cuando el empleador: utiliza datos para fines ajenos a la relación laboral, difunde información sensible sin autorización, implementa mecanismos de vigilancia desproporcionados, emplea datos para represalias, discriminación u hostigamiento. En tales supuestos, la autoridad inspectiva puede imponer sanciones administrativas, sin perjuicio de la competencia concurrente de la ANPDP, configurándose un sistema de tutela administrativa complementaria.

5.4. MINISTERIO DE TRABAJO Y GOBERNANZA INSTITUCIONAL

El Ministerio de Trabajo y Promoción del Empleo aborda la protección de datos desde una perspectiva de gobernanza organizacional, mediante políticas internas de seguridad de la información alineadas con la LPDP y las directivas de la ANPDP. Su enfoque se sustenta en: Políticas específicas de seguridad, difusión permanente, evaluación continua de controles, actualización normativa interna, capacitación del personal y cooperación con trabajadores y representantes. Este modelo consolida la protección de datos como un componente estructural de la gestión pública moderna y del respeto a la dignidad laboral.

5.5. TUTELA JUDICIAL: EL HÁBEAS DATA

En el ámbito jurisdiccional, la protección de los datos personales se garantiza principalmente mediante el proceso constitucional de hábeas data, regulado en el Código Procesal Constitucional, a través de los Juzgados y Salas Constitucionales de la Corte

Superior de Justicia, así como el Tribunal Constitucional. Este proceso tutela: a) El derecho de acceso a la información pública y, b) El derecho a la autodeterminación informativa. Su sustento constitucional se encuentra en los artículos 2 incisos 6 y 7, así como en los artículos 201 y 202 de la Constitución Política del Perú. Entre sus principales características destacan: Gratuidad y celeridad, accesibilidad procesal, facultad de corrección, actualización o supresión de datos, tutela rápida y efectiva. El hábeas data consolida la autodeterminación informativa como un derecho operativo, exigible y justiciable.

5.6. VALORACIÓN CRÍTICA

La multiplicidad de actores institucionales demuestra que la protección de datos personales en el Perú no es un problema exclusivamente normativo, sino esencialmente institucional y estructural. La eficacia del sistema depende de la articulación real entre autoridades administrativas, órganos inspectivos, entidades sectoriales y el Poder Judicial. Sin embargo, sin coordinación efectiva, cultura de cumplimiento y ciudadanía informada, la protección de datos corre el riesgo de convertirse en un derecho formal sin tutela material, especialmente en un contexto marcado por la inteligencia artificial, el big data y la economía digital.

6. DESAFÍOS EN LA PROTECCIÓN DE DATOS Y LOS DERECHOS FUNDAMENTALES ANTE LA INTELIGENCIA ARTIFICIAL

El primer gran desafío consiste en la insuficiencia de una regulación laboral específica sobre el uso de la inteligencia artificial en el tratamiento de datos personales de los trabajadores. Si bien la Ley No. 29733 establece principios generales de protección, estos resultan limitados para abordar fenómenos complejos como la toma de decisiones automatizadas, la elaboración de perfiles, la supervisión algorítmica y la evaluación predictiva del desempeño, lo que genera vacíos normativos e interpretativos que debilitan la

tutela efectiva de la autodeterminación informativa en el ámbito laboral.

Un segundo reto relevante radica en la profunda asimetría técnica, informativa y cognitiva entre empleador y trabajador respecto del funcionamiento de los sistemas algorítmicos. La opacidad de los modelos de inteligencia artificial impide al trabajador conocer los criterios, variables y ponderaciones utilizadas en las decisiones que inciden directamente en su acceso, permanencia o promoción en el empleo, afectando gravemente los principios de transparencia, debido proceso y no discriminación.

No obstante, el desafío más crítico es la progresiva normalización de la vigilancia laboral mediante mecanismos de control digital permanente, tales como la geolocalización, la videovigilancia, el análisis de productividad y el monitoreo conductual mediante inteligencia artificial. Estas prácticas corren el riesgo de transformar el poder de dirección empresarial en un sistema de control estructural incompatible con la dignidad humana y con el modelo constitucional de relaciones laborales. Frente a ello, resulta indispensable garantizar estándares de transparencia, trazabilidad, explicabilidad y revisión humana en los procesos automatizados, de modo que la inteligencia artificial sea utilizada de forma ética, proporcional y jurídicamente responsable.

7. CONCLUSIONES

A manera de conclusión, consideramos que la protección de los datos personales en el ámbito laboral impone al empleador el deber de actuar como garante de la información personal de sus trabajadores, asegurando su registro, seguridad, confidencialidad y uso legítimo, especialmente en un contexto en el que la digitalización y la inteligencia artificial influyen de manera decisiva en los procesos de selección, evaluación y gestión del talento humano. En tal sentido, la aplicación de inteligencia artificial en la gestión laboral exige una reinterpretación del poder de dirección del empleador, el cual debe ser comprendido

como una función jurídicamente limitada por los principios de proporcionalidad, finalidad, transparencia y respeto a los derechos fundamentales del trabajador.

Por otro lado, señalar que la tutela de los datos personales del trabajador no es un aspecto accesorio, sino un componente estructural del trabajo decente y de la gobernanza responsable en entornos digitales, en tanto garantiza la dignidad, la igualdad de oportunidades y la autodeterminación informativa frente a tratamientos masivos y automatizados.

Finalmente, se concluye que el ordenamiento peruano requiere una evolución normativa, jurisprudencial e institucional que incorpore de manera expresa los impactos de la inteligencia artificial en el ámbito laboral, mediante reglas claras sobre decisiones automatizadas, auditoría algorítmica, transparencia, responsabilidad empresarial y fortalecimiento de los mecanismos de tutela administrativa y judicial, a fin de asegurar una protección efectiva de los derechos fundamentales en la era digital y en el marco del trabajo decente.

BIBLIOGRAFÍA

- Aguilera Izquierdo, R., “El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización.” *Revista de Trabajo y Seguridad Social*. CEF, (442), 2020, 93–134. <https://doi.org/10.51302/rtss.2020.886>
- Alvarado, F. J., “La gestión de la seguridad de la información en el régimen peruano de protección de datos personales.” *Foro Jurídico*, (15), 2016, 26–41. <https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19833>
- Blancas Bustamante, C., “Poder de dirección y derecho a la intimidad y privacidad del trabajador.” *Revista de la sociedad peruana de derecho del trabajo y de la seguridad social*. 2021, Pp. 157-184. <https://www.sptss.org.pe/wp-content/uploads/2021/09/Laborem10-147-174.pdf>
- Blume Moore, I., “Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales”. *Themis*

- Revista de Derecho*, (79), 2021, 435-449. <https://doi.org/10.18800/themis.202101.025>
- Castro Cruzatt, K, “El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú”. *Ius et Veritas*, 2008. Revista No.37. Pp. 260-276<https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/12229/12795>
- Cerda Silva, A., “Autodeterminación informativa y leyes sobre protección de datos”. *Revista chilena de derecho informático*. 2003, Pp. 47-75. https://www.researchgate.net/profile/Alberto-Cerda-Silva/publication/273029066_Autodeterminacion_informativa_y_leyes_sobre_proteccion_de_datos/links/5ad345aeaca272fdaf7a4561/Autodeterminacion-informativa-y-leyes-sobre-proteccion-de-datos.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail&_rtd=e30%3D
- Champi Zavaleta, L; del Águila Rodríguez, B; García Martínez, A; Meneses Oriundo, Y., “Análisis de la eficacia normativa de la Ley de Protección de Datos Personales en el sector empresarial financiero: Propuesta de mejora del marco normativo para el fortalecimiento de la Ciberseguridad Corporativa”. Trabajo de Suficiencia Profesional presentado en satisfacción parcial de los requerimientos para obtener el Título Profesional de Abogado. Facultad de Derecho y Ciencias Sociales. Universidad ESAN. 2025, Páginas 1-89. <https://repositorio.esan.edu.pe/server/api/core/bitstreams/c04be726-744a-436d-bba9-798046ccf83c/content>.
- Conde Ortiz, C., “La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad”. Universidad de Cádiz. Editorial Dykinson, S.L. Madrid. España, 2005, Pp. 01-118. <https://rodin.uca.es/handle/10498/26396>
- Corrales Melgarejo, E. R., “Entre los derechos a la intimidad y protección de los datos personales en el trabajo y el poder fiscalizador del empleador: las cámaras de video-

- vigilancia.” *Revista oficial del poder judicial*, 15(19), 2023, 261-277. <https://doi.org/10.35292/ropj.v15i19.739>
- Cubillos Vélez. A., “La explotación de los datos personales por los gigantes de internet”. *Revista de la Biblioteca Jurídica Virtual* del Instituto de Investigaciones Jurídicas de la UNAM, 2017, Pp. 27-55. <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>
- Duffy, P, Zegarra, J & Tolentino, C., “Protección de datos personales: ¿Cuándo se vulnera el derecho a los trabajadores?”, *Artículos Dentons*. 2025. <https://www.dentons.com/es/insights/articles/2025/march/25/cuando-se-vulnera-el-derecho-a-los-trabajadores>
- Franco García, D., & Quintanilla Perea, A., “La protección de datos personales y el derecho al olvido en el Perú”. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Derecho PUCP*, (84), 2020, páginas 271–299. <https://doi.org/10.18800/derechopucp.202001.009>
- López Ahumada, J. E., “El desarrollo de los estándares de protección de la intimidad en el ámbito laboral desde la perspectiva de la tutela de los derechos fundamentales”. *Derechos Fundamentales y Derecho del Trabajo ante el Proceso de Transformación Digital*. Universidad de Alcalá. Departamento de Ciencias Jurídicas. Lucerna Juris. Primera Edición 2024. Pp. 127-142. <https://dialnet.unirioja.es/servlet/libro?codigo=1006429>
- Lopez Ahumada, J.E., “Transformación digital y su repercusión en los derechos fundamentales de las personas trabajadoras”. *Preámbulo. Derechos Fundamentales y Derecho del Trabajo ante el Proceso de Transformación digital*. Universidad de Alcalá. Departamento de Ciencias Jurídicas. Lucerna Juris. Primera Edición 2024. Pp. 7-13. <https://dialnet.unirioja.es/servlet/libro?codigo=1006429>
- Lora, G., “Protección de datos personales y procesos judiciales de naturaleza laboral.”, 2025. Consultada el 18 de enero del

2026. <https://aperhu.pe/proteccion-de-datos-personales-y-procesos-judiciales-de-naturaleza-laboral/>
- Martínez Martínez, R., “El derecho fundamental a la protección de datos: perspectivas.” Monográfico III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas. *Revista de internet, derecho y política*. No. 5. Universitat Oberta de Catalunya, 2007, Pp. 47-61. <https://www.redalyc.org/pdf/788/78812861005.pdf>
- Olivos Celis, M., “El camino del derecho a la protección de datos personales en el Perú tras su incorporación en la constitución política de 1993”. *Ius Revista de Investigación* de la Facultad de Derecho. 2020. Universidad Católica Santo Toribio de Mogrovejo-Chiclayo, Perú. US Vol. 9. No. 1. P. 89. <http://doi.org/10.35383/ius-usat.v9i1.338>
- Palomeque López, M., “Los derechos laborales en la Constitución Española. Madrid. Centro de Estudios Constitucionales.”, 1991.
- Palomeque López, M y Álvarez de la Rosa, M., “Derecho del trabajo”. Novena ed. Madrid. Centro de Estudios Ramón Areces S.A, 2001.
- Puntriano Rosas, C., “Apuntes sobre la protección de datos personales en la relación laboral en el Perú”. *Pareceres Revista Derecho del Trabajo*. Año X. No. 37. 2022, Pp. 189-206. https://www.munizlaw.com/assets/pdf/RDT_37_UY_art_cpr_con_car%C3%A1tula.pdf
- Ramírez Rondán, E., “Programa de Segunda Especialidad en Derecho del Trabajo y de la Seguridad Social. El deber de protección del empleador sobre los datos personales en las relaciones laborales entre trabajadores”. Trabajo académico para optar el título de Segunda Especialidad en Derecho del Trabajo y de la Seguridad Social. Facultad de Derecho de la Pontificia Universidad Católica del Perú – PUCP, 2023. Pp. 01-40. <https://tesis.pucp.edu.pe/server/api/core/bitstreams/6e547f68-3ec8-4553-995c-d1a91ef0a48c/content>
- Torres Montano, R., “Gobierno digital y protección de datos perso-

- nales en la administración pública peruana”. *Revista Sapere* Facultad de Derecho –USMP. Vol. 1 Núm. 28. 2025, Pp. 1-16. <https://portalrevistas.aulavirtualusmp.pe/index.php/SP/article/view/3271/4039>
- Trillo Vigil, C., “Compliance laboral en materia de protección de datos personales”. Trabajo de investigación para optar el grado académico de magíster en derecho de la empresa. Pontificia Universidad Católica del Perú. Escuela de posgrado., 2019, Pp. 1-55. <https://tesis.pucp.edu.pe/server/api/core/bitstreams/afe20596-3ab7-4a7f-8766-f121a-07f0a84/content>
- Urrutia Zamalloa, J. & Valencia Castillo, R., "La protección de datos personales de los trabajadores frente al uso de tecnologías de monitoreo GPS y videovigilancia en el entorno laboral". Trabajo de Suficiencia Profesional presentado en satisfacción parcial de los requerimientos para obtener el título profesional de Abogado. Universidad ESAN, 2024, Pp. 1-61. <https://repositorio.esan.edu.pe/server/api/core/bitstreams/421ced9b-0f71-40e0-9549-729f35d4893d/content>
- Zamudio Salinas, M., “El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. límites y propuestas”. Tesis para optar el grado académico de Magíster en Derecho con mención en Derecho Constitucional, 2021, Pp. 1-225 <https://tesis.pucp.edu.pe/server/api/core/bitstreams/a574e4d8-a030-4192-97d4-3f7bdf5ee22a/content>
- Zamudio Salinas, M., “Perú: retos del derecho fundamental a la protección de datos”. *Revista peruana de derecho constitucional*, N° 15, enero-junio, 2023, Pp. 327-343 <https://revista.tc.gob.pe/index.php/revista/article/view/406/414>.

Páginas web consultadas:

Agencia Española de Protección de Datos (AEPD), Protección de Datos: Guía para el ciudadano. Agencia Española de Protección de Datos. 2018. <https://www.aepd.es/guias/guia-ciudadano.pdf>

- Ley de protección de datos personales LEY N °29733 <https://cdn.www.gob.pe/uploads/document/file/2011398/Ley%20N%C2%BA%2029733%20-%20Ley%20de%20protecci%C3%B3n%20de%20datos%20personales.pdf?v=1683928275>
- Decreto Supremo que aprueba el Reglamento de la Ley No. 29733, Ley De Protección De Datos Personales <https://cdn.www.gob.pe/uploads/document/file/7756037/6554453-reglamento-de-la-ley-n-29733.pdf?v=1743779969>
- Constitución Política del Perú, Ministerio de Justicia y Derechos Humanos, Vigésima edición oficial. 2025, Pp. 27-30. <https://cdn.www.gob.pe/uploads/document/file/8775223/7255126-vigesima-constitucion-2025-08-25.pdf?v=1759507534>
- Código Penal Peruano, Ministerio de Justicia y Derechos Humanos. Décimo Segunda Edición Oficial, 2016, P. 111. <https://cdn.www.gob.pe/uploads/document/file/3621138/C%C3%93DIGO%20PENAL.pdf?v=1663014332>
- Directiva No. 01-2020-JUS/DGTAIPD, Plataforma del Estado Peruano. 2020, Pp. 1-24 <https://cdn.www.gob.pe/uploads/document/file/1910249/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf?v=1621961664>
- Ley No. 31814, Ley Marco de Desarrollo de la Inteligencia Artificial. Plataforma del Estado Peruano, 2023, Pp. 1-3 <https://cdn.www.gob.pe/uploads/document/file/5038703/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814.pdf?v=1692895308>
- Decreto Legislativo No. 1353, crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de Intereses. Plataforma del Estado Peruano. 2017, Pp. 1-7 <https://cdn.www.gob.pe/uploads/document/file/2790446/Decreto%20Legislativo%20N%C2%BA%201353.pdf?v=1643321801>
- Decreto de Urgencia No. 007-2020, que aprueba el Marco de

Confianza Digital (2020). Plataforma del Estado Peruano. 2020, Pp. 1-4 <https://cdn.www.gob.pe/uploads/document/file/2790485/Decreto%20de%20Urgencia%20N%C2%BA%20007-2020.pdf?v=1643322610>

Decreto Legislativo No. 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital (2018). Plataforma del Estado Peruano. Pp. 1-5 <https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf?v=1566312763>

STC Exp. No. 1797-2002-HD/TC <https://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html>

STC No. 00141-2011-PA/TC <https://www.tc.gob.pe/jurisprudencia/2011/00141-2011-AA%20Resolucion.html>